明 細 書

# セキュアシステム、セキュアデバイス、端末装置、方法およびプログラム

## 技術分野

[0001] 本発明は、端末装置とセキュアデバイスとを含むセキュアシステムであって、例えば、複数のコンテンツ利用装置およびICカードからなるコンテンツまたはライセンスを共有可能な範囲であるドメイン内外でのコンテンツの利用制御をおこなうコンテンツ利用システム、ICカード、コンテンツ利用装置、方法およびプログラムに関する。

## 背景技術

[0002] 現行のデジタル放送において、有料放送を契約した会員だけにコンテンツを提供するため、ハードウェア的に耐タンパ化されたセキュリティ・モジュール(例えばICカード)を用いて、コンテンツの利用を制御するコンテンツ利用システムがある。このようなシステムでは、ICカードは、暗号化コンテンツを復号するために必要な暗号鍵をセキュアに格納し、限定された1台のコンテンツ利用装置においてコンテンツの復号を可能にする「ペアリング」とよばれる技術がしばしば用いられる。しかし、このようなコンテンツ利用システムにおいては、会員が複数台のコンテンツ利用装置を所有している場合に、特定の1台でしかICカードが使用できないので、不便である。これは、例えば、コンテンツをいったんハードディスク等に蓄積して、会員が所望する時間に視聴する放送形態(サーバ型放送と呼ぶ。)においても、特定の1台のコンテンツ利用装置でしかICカードが使用できないと不便である。なお、サーバ型放送規格については、ARIB(Association of Radio Industries and Businesses)により発行されているSTD－B25などが詳しい。

[0003] また、日本における現行BS／CS／地上デジタル放送では、ICカードとコンテンツ利用装置はペアリングされておらず、ICカードはどのコンテンツ利用装置であっても利用可能である。しかし、多様なサービスを提供可能なサーバ型放送などにおいては、ICカードが利用可能なコンテンツ利用装置を限定したい、というニーズは大きいと考えられる。

[0004] このような背景から、複数台のコンテンツ利用装置でICカードを共用するコンテンツ

利用システムが提案されている。例えば、特許文献1に開示されたコンテンツ利用システムでは、ICカードを共用する複数のコンテンツ利用装置と複数のICカードとからなるグループ(以降、ドメインと呼ぶ。)には共通の識別子が割り当てられ、コンテンツ利用装置は同じ識別子が割り当てられたICカードを利用することができる。

特許文献1:特表2001－518255号公報

## 発明の開示

### 発明が解決しようとする課題

[0005] しかしながら、上記従来技術によれば、ICカードをドメイン外のコンテンツ利用装置で使用することができないので、ユーザの利便性が悪い場合が発生しうる。例えば、ユーザが友人宅にICカードを持って行った場合に、友人宅のコンテンツ利用装置では、そのICカードを一時的にでも一切使用するということができないので、極めて利便性が悪くなってしまう。

[0006] つまり、ICカードは、そのICカードと同じドメイン以外に属するコンテンツ利用装置に挿入しても、そのコンテンツ利用装置でコンテンツを再生することができない。

[0007] 上記課題に鑑み、本発明は、コンテンツなどの秘匿データの保護を考慮しつつ、ドメイン外のコンテンツ利用装置においてもセキュアデバイスを利用可能にすることで、秘匿データの保護とユーザ利便性の両者のバランスをとるセキュアシステム、セキュアデバイス、コンテンツ利用装置、方法およびプログラムを提供することを目的とする。

### 課題を解決するための手段

[0008] 上記目的を達成するため、本発明のセキュアシステムは、秘匿データを保持するセキュアデバイスと、セキュアデバイスを接続する端末装置とを含むセキュアシステムであって、セキュアデバイスおよび端末装置の何れかに備えられ、セキュアデバイスおよび端末装置のドメインを定義するドメイン情報とを記憶する第1記憶手段と、セキュアデバイスおよび端末装置の何れかに備えられ、ドメイン外におけるセキュアデバイスの利用条件であるドメイン外利用条件を記憶する第2記憶手段と、セキュアデバイスおよび端末装置の何れかに備えられ、前記ドメイン情報に従ってセキュアデバイスまたは端末装置が現在ドメイン内であるかドメイン外であるかを判定する第1判定手

段と、セキュアデバイスおよび端末装置の何れかに備えられ、第1判定手段によってドメイン外であると判定されたとき、前記ドメイン外利用条件に従ってセキュアカードの利用可否を判定する第2判定手段と、セキュアデバイスおよび端末装置の何れかに備えられ、第1判定手段によってドメイン内と判定された場合、および、第2判定手段によって利用可能と判定された場合に、端末装置によるセキュアデバイスの利用を可能にする制御手段とを備える。

[0009] この構成によれば、ドメイン外でのセキュアデバイスの利用条件を示すドメイン外利用条件の範囲内でセキュアデバイスをドメイン外のコンテンツ利用装置でも使用することができるので、ユーザの利便性を向上させることができる。しかも、ドメイン外でのセキュアデバイスの使用は無制限ではなく、ドメイン外利用条件によって限定されるので、コンテンツなどの秘匿データの保護を図ることができる。

[0010] ここで、前記第1記憶手段はセキュアデバイスに備えられ、前記第1判定手段は、端末装置に備えられ、当該端末装置が現在ドメイン内であるかドメイン外であるかを判定し、前記制御手段はセキュアデバイスに備えられるようにしてもよい。

[0011] ここで、前記端末装置は、暗号化されたコンテンツを再生するコンテンツ利用装置であり、前記秘匿データは前記コンテンツを復号するための暗号鍵であり、前記制御手段は、セキュアデバイスに備えられ、第1判定手段によってドメイン内と判定された場合、および、第2判定手段によって利用可能と判定された場合に、セキュアデバイスから端末装置に前記秘匿データを供給するようにしてもよい。

[0012] ここで、前記ドメイン外利用条件は、ドメイン外での(a)コンテンツ再生の回数、(b)コンテンツ利用装置の台数、(c)ドメイン数、(d)有効期限、(e)利用時間、(f)端末ID数、(g)ドメインID数、(h)コンテンツの数および(i)ライセンスの数、の少なくとも1つに関するようにしてもよい。

[0013] この構成によれば、ドメイン外利用条件として、例えば、ドメイン外では3回までコンテンツを利用可能であるとか、ドメイン外のコンテンツ利用装置は2台(2つの端末ID)まで利用可能であるとか、ドメイン外でのコンテンツ利用は1つまでであるとか、ドメイン外では4月1日まで使用可能であるとか、ドメイン外では2週間使用可能であるとか、ドメイン外では4月6日から使用可能であるとか、ドメイン外では1つのドメインIDに

限定するとか、コンテンツ2種類まで、ライセンス(暗号鍵)2つまで等のドメイン外利用条件を設定することができるので、事業者の意向やコンテンツの特性に応じた利用条件を設定することによって、事業者の権利保護とユーザの利便性を十分に調整することができる。

[0014] ここで前記セキュアデバイスは、ドメイン外のコンテンツ利用装置における前記ドメイン外利用条件に基づくコンテンツの利用履歴を示すドメイン外利用履歴を記録する履歴記録手段を備え、前記第2判定手段は、前記ドメイン外利用履歴が前記利用条件に示される利用可能な範囲を超えないか否かを判定するようにしてもよい。

[0015] この構成によれば、第2判定手段はドメイン外での利用履歴(以下、ドメイン外利用履歴)とドメイン外利用条件に示される利用可能な範囲とを比較することにより容易に判定することができる。

[0016] ここで、第2記憶手段および第2判定手段は、前記セキュアデバイスに備えられる構成としてもよい。

[0017] この構成によれば、セキュアデバイス自身が利用可否を判定し、セキュアデバイス内にドメイン外利用履歴を記録するので、コンテンツ利用装置はほぼ従来の構成であっても利用することができる。また、ICカードなどのセキュアデバイスはハードウェアレベルで耐タンパ化されているので、セキュリティレベルをより向上させることができる。さらに、ICカードを新しいICカードに交換することにより、ドメイン外利用条件などを含めたセキュリティの更新が可能となる。

[0018] ここで、第2記憶手段および第2判定手段は、前記コンテンツ利用装置に備えられる構成としてもよい。

[0019] この構成によれば、コンテンツ利用装置自身が利用可否を判定し、ドメイン外利用履歴を記録するので、セキュアデバイスはほぼ従来の構成であっても利用することができる。

[0020] ここで、前記セキュアデバイスは、さらに、所定の時期に前記ドメイン外利用履歴を消去する消去手段を備えてもよい。

[0021] ここで、前記消去手段は、セキュアデバイスが特定のドメイン内の何れかの前記コンテンツ利用装置のセキュアデバイススロットに挿入されたとき、前記ドメイン外利用履

歴を消去するようにしてもよい。

[0022] ここで、前記消去手段は、前記セキュアデバイスが特定のドメイン内の特定のコンテンツ利用装置のセキュアデバイススロットに挿入されたとき、前記ドメイン外利用履歴を消去するようにしてもよい。

[0023] この構成によれば、利用条件に示される利用可能な範囲を全て使用した場合などに、ユーザは再度ドメイン外利用履歴を初期化(リセット)することができる。

[0024] ここで、前記消去手段は、コンテンツ利用装置から消去指示を受信したとき、前記ドメイン外利用履歴を消去するようにしてもよい。

[0025] この構成によれば、コンテンツ利用装置においてドメイン外利用履歴を初期化することを制御することができる。

[0026] ここで、前記コンテンツ利用装置は、外部から前記ドメイン外利用履歴の消去指示を受信し、セキュアデバイススロットに挿入されている同一ドメイン内のセキュアデバイスに当該消去指示を送信するようにしてもよい。

[0027] この構成によれば、例えば、事業者つまりコンテンツ配信装置がドメイン外利用履歴の初期化を制御することにより、ドメイン外でのセキュアデバイスの利用をきめ細かく制御することができる。

[0028] ここで、前記コンテンツ利用端末は、外部から新たなドメイン外利用条件を受信する受信手段を備え、前記第2記憶手段は、前記ドメイン外利用条件を新たなドメイン外利用条件に更新するようにしてもよい。

[0029] この構成によれば、例えば、事業者つまりコンテンツ配信装置が、利用条件の内容を自由に制御することにより、ドメイン外でのセキュアデバイスの利用を動的に、きめ細かく制御することができる。

[0030] ここで、前記受信手段は、コンテンツ配信サーバから送信されるライセンスに付加されたドメイン外利用条件を受信するようにしてもよい。

[0031] この構成によれば、ライセンス毎にコンテンツやライセンスの特性に適したドメイン外利用条件を設定することができる。

[0032] ここで、第2記憶手段は、デフォルトのドメイン外利用条件を記憶するようにしてもよい。

[0033] この構成によれば、ドメイン外利用条件を事後的に設定する処理を行うことなく、工場出荷時に予め利用条件をセキュアデバイスに記憶させることができる。

[0034] ここで、前記コンテンツ利用装置は、さらに、セキュアデバイススロットに挿入されたセキュアデバイスからドメイン外利用条件およびドメイン外利用履歴を取得する取得手段と、取得したドメイン外利用条件およびドメイン外利用履歴に基づいてドメイン外のコンテンツ利用装置における利用状況に関するガイダンスを表示する表示手段とを備えるようにしてもよい。

[0035] この構成によれば、ユーザはガイダンス表示によって利用状況を把握することができる。

[0036] ここで、前記表示手段は、前記ドメイン外利用履歴が前記ドメイン外利用条件に示される利用可能範囲に達しているとき、前記ドメイン外利用履歴の消去を促すガイダンスを表示するようにしてもよい。

[0037] この構成によれば、ドメイン外のコンテンツ利用装置ではもはや使用できなくなった場合に、使い慣れないユーザでも対処することができる。

[0038] ここで、前記表示手段は、前記ドメイン外利用履歴の消去方法を示すヘルプメッセージを前記ガイダンスとして表示するようにしてもよい。

[0039] この構成によれば、ドメイン外のコンテンツ利用装置ではもはや使用できなくなった場合に、使い慣れないユーザでも消去のための具体的な行動をすることができる。

[0040] ここで、前記表示手段は、前記ドメイン外利用履歴と前記ドメイン外利用条件に示される利用可能範囲との差分が一定以下のとき、その旨を前記ガイダンスとして表示するようにしてもよい。

[0041] この構成によれば、ドメイン外のコンテンツ利用装置では使用できなる前に、ユーザに対して警告することができる。

[0042] ここで、前記コンテンツ利用装置は、さらに、セキュアデバイススロットに挿入されたセキュアデバイスから前記ドメイン外利用条件および前記ドメイン外利用履歴を取得する取得手段と、取得した前記ドメイン外利用条件および前記ドメイン外利用履歴に基づいてドメイン外のコンテンツ利用装置における利用状況に関するガイダンスを表示する表示手段とを備えるようにしてもよい。

[0043] この構成によれば、ドメイン外のコンテンツ利用装置ではもはや使用できなくなった場合に、その旨を警告するので、ユーザがセキュアデバイスの故障などと勘違いすることを防止することができる。

[0044] また、本発明のセキュアデバイス、コンテンツ利用装置、コンテンツ利用方法、プログラムについても上記と同様の作用・効果を奏する。

## 発明の効果

[0045] 本発明のセキュアシステム、セキュアデバイス、コンテンツ利用装置、コンテンツ利用方法、プログラムによれば、利用条件の範囲内でドメイン外のコンテンツ利用装置においてもセキュアデバイスを利用可能にする。よって、コンテンツなどの秘匿データの保護を考慮しつつ、秘匿データの保護とユーザ利便性の両者のバランスをとることができる。

## 図面の簡単な説明

[0046] [図1]図1は、本発明の実施形態1におけるコンテンツ利用システムの概要を示す図である。

[図2]図2は、本コンテンツ利用システムの全体の構成を示すブロック図である。

[図3]図3は、コンテンツ蓄積部に蓄積されるコンテンツの一例を示す図である。

[図4]図4は、ライセンス情報蓄積部に蓄積されるライセンス情報例を示す図である。

[図5]図5は、ドメイン外利用条件蓄積部に蓄積される利用条件例を示す図である。

[図6]図6は、ドメイン情報蓄積部に蓄積されるドメイン情報例を示す図である。

[図7]図7は、EMMのデータ例を示す図である。

[図8]図8は、端末ID保持部のデータ例を示す図である。

[図9]図9は、ドメイン情報保持部に保持されるドメイン情報例を示す図である。

[図10]図10は、ドメイン外利用条件保持部に保持されるドメイン外利用条件例を示す図である。

[図11]図11は、ドメイン外利用記録蓄積部に蓄積される利用記録例を示す図である。

[図12]図12は、ドメイン外利用条件のICカードへの設定処理についてのフローチャートを示す図である。

[図13]図13は、コンテンツ再生処理についてのフローチャートを示す図である。

[図14]図14は、ドメイン外利用記録の消去処理についてのフローチャートを示す図である。

[図15]図15は、本発明の実施形態2におけるセキュアシステムの概要を示す図である。

[図16]図16は、端末装置Taとメモリカードの構成を示すブロック図である。

[図17]図17は、ドメイン情報保持部に保持されるドメイン情報の例を示す図である。

[図18]図18は、ドメイン情報保持部に保持されるドメイン情報の他の例を示す図である。

符号の説明

[0047]

100 配信装置

101 コンテンツ蓄積部

102 ライセンス情報蓄積部

103 ドメイン外利用条件蓄積部

104 ドメイン外利用条件付加部

105 ドメイン情報蓄積部

106 端末リスト付加部

107 EMM生成部

108 放送信号多重送信部

200 端末装置

201 放送信号受信分離部

202 コンテンツ記憶部

203 再生部

204 EMM取得部

205 端末ID読み出し部

206 端末ID保持部

207 ドメイン外利用条件取り出し部

208 第1の送受信部

300 ICカード

301 第2の送受信部

302 ドメイン情報保持部

303 端末ID取得部

304 ドメイン情報処理部

305 ドメイン外利用条件保持部

306 ドメイン外利用条件取得部

307 ドメイン外利用記録蓄積部

308 ドメイン外利用記録更新部

309 ドメイン外利用可否判定部

## 発明を実施するための最良の形態

[0048] 本発明のセキュアシステムは、秘匿データを保持するセキュアデバイスと、セキュアデバイスを利用する複数の端末装置とを含む。ユーザがドメイン内の端末装置だけでなく、条件付きではあるけれどもドメイン外の端末装置でもセキュアデバイスを利用できるように構成されている。ここで、ドメインとは、ライセンスおよびコンテンツを共用する端末装置およびセキュアデバイスの集合をいう。ユーザがドメインAに属するセキュアデバイスをドメインAに属する端末装置に接続した場合は、当該端末装置は無条件でセキュアデバイスを利用できるだけでなく、ドメインBに属する端末装置に接続した場合でも、当該端末装置がドメイン外利用条件の範囲内でセキュアデバイスを利用できるように構成されている。実施の形態1では、セキュアシステムとしてコンテンツ利用システムを、セキュアデバイスとしてICカードを例にとって説明する。

[0049] (実施の形態1)

図1は、本発明の実施の形態1におけるコンテンツ利用システムの概要を示す図である。同図のように、本コンテンツ利用システムは、放送局100、端末装置200a～200c、端末装置200p、200q、セキュアデバイスとしてICカード300a～300cを含み、ユーザがドメイン内の端末装置だけでなく、条件付でドメイン外の端末装置でICカードを使用してコンテンツを視聴できるように構成されている。例えば、ユーザがドメインAに属するICカード300aを、ドメインBに属する端末装置200pに挿入した場合に、

ドメイン外利用条件の範囲内で端末装置200pがコンテンツを再生できる。

[0050] 図2は、コンテンツ利用システムの全体構成を示すブロック図である。同図のように、本コンテンツ利用システムは、配信装置100、端末装置200、ICカード300を含む。

[0051] 配信装置100は、図1における放送局100に相当し、コンテンツプロバイダやサービスプロバイダと呼ばれる事業者であり、限定受信方式および限定再生方式によるサーバ型放送によりセキュアにコンテンツを放送する。この配信装置100は、コンテンツ蓄積部101、ライセンス情報蓄積部102、ドメイン外利用条件蓄積部103、ドメイン外利用条件付加部104、ドメイン情報蓄積部105、端末リスト付加部106、EMM生成部107、放送信号多重送信部108を備える。

[0052] コンテンツ蓄積部101は、図3に示すようなコンテンツデータ3000を蓄積する。図3に示すように、コンテンツデータ3000は、コンテンツID3001と、メタデータ3002と、暗号化コンテンツ3003とから成る。コンテンツID3001は、デジタルコンテンツ配信システム内において、コンテンツを一意に特定するためのIDである。メタデータ3002は、コンテンツの内容を説明するデータであり、コンテンツのタイトルやコンテンツの長さ等が記述されている。暗号化コンテンツ3003は、音楽データや映像データ等のコンテンツを暗号化したものである。なお、コンテンツは、音楽データや映像データに限られたものではなく、電子新聞、電子ブック、電子マップ、電子辞書、静止画、ゲーム、コンピュータ用ソフトウェア等のデジタルコンテンツであってもよい。

[0053] ライセンス情報蓄積部102は、図4に示すようなコンテンツの再生に必要なライセンス400と、暗号化されたライセンス400の復号に必要なワーク鍵と呼ばれる暗号鍵とを蓄積する。図4に示すように、ライセンス400は、ドメイン内の端末装置200に対するコンテンツの利用条件を示す利用条件401と、ライセンス400に対応する暗号化コンテンツの復号を行うためのコンテンツ鍵402と、ライセンス400を共用してよいドメインを特定するドメインID403と、からなる。ここで、利用条件401の一例としては、ライセンス400に対応するコンテンツを利用可能な回数(例えば「10回」)や、利用可能な期間(例えば「2004年4月1日～2004年5月30日」)などである。なお、同図において、ライセンス400は、ドメインID403を含む代わりに、あるいはドメインID403と併せて、それぞれユーザ、端末装置、ICカードを一意に識別可能な、ユーザID、端末装

置ID、ICカードIDを含むようにしてもよい。なお、ライセンス400は、コンテンツID3001と関連付けるため、ライセンス400にコンテンツID3001を含めてもよい。ライセンス400にコンテンツID3001を含める代わりに、ライセンス400を一意に特定するためのライセンスIDなどの識別子をライセンス400に含めるようにしてもよい。また、ワーク鍵は、事業者と関連付けて蓄積され、定期的にEMMなどにより更新される。

[0054] ドメイン外利用条件蓄積部103は、図5に示すような、ドメイン外の端末装置に対する複数のドメイン外利用条件をドメイン外利用条件テーブル500として蓄積する。図5に示すように、ドメイン外利用条件テーブル500は、ユーザID501とドメイン外利用条件502とを対応付けて蓄積する。ユーザID501は、本コンテンツ配信システム内において、ユーザを一意に特定するIDである。ユーザID501は、コンテンツ配信サービスを受けるために、事業者に会員登録処理をする際に割り当てられる。この会員登録処理は、ユーザが、ネットワーク上で事業者と通信して行われてもよいし、会員登録用書類の送付等、他の方法で行われてもよい。会員登録処理では、まず、事業者が、ユーザに対してユーザID501を割り当てる。その後、ユーザが所有する端末装置200の端末IDが、ネットワークもしくは書類等により事業者に対して通知される。この通知された端末IDとユーザID501とが関連付けられて管理される。また、ICカードID、ドメインIDの割り当ても同様にして、会員登録後随時行われる。ドメイン外利用条件502は、ICカード300をドメイン外の端末装置で使用する条件を定め、コンテンツ再生の回数、利用可能なドメイン外のコンテンツ利用装置の台数、利用可能なドメイン数、有効期限、有効期間、発効時期、最大の利用時間、端末ID数、ドメインID数、コンテンツの数、ライセンス(コンテンツ鍵)の数、などをドメイン外利用条件として定める。例えば、ユーザID「USER－ID－0001」で特定されるユーザに対して「使用可能な端末装置の端末IDが3つまで許可」というドメイン外利用条件502が与えられている。また、ユーザID「USER－ID－0002」で特定されるユーザに対して、「3つ(回)まで許可」というドメイン外利用条件が与えられている。ユーザID「USER－ID－0003」で特定されるユーザに対して「初回利用から1ヶ月経過後無効」、すなわち、ある端末で最初に利用してからドメイン外で1ヶ月間は有効、というドメイン外利用条件502が与えられている。このドメイン外利用条件に示される利用範囲内で、ユーザ

は、所有しているICカードのドメイン外の端末装置でも、コンテンツを利用することが可能になる。なお、ドメイン外利用条件は複数の条件を含んでいてもよい。その場合、ドメイン外利用条件による利用可否は、複数の条件のAND(複数の条件を全て満たす場合に利用可能)やOR(複数の条件のいずれかを満たす場合に利用可能)により判定してもよい。

[0055] ドメイン外利用条件付加部104は、EMM生成部107によって生成されるEMM(Entitlement Management Message)にドメイン外利用条件502を付加する。ここでEMMは、ユーザとの個別の契約情報やコンテンツ鍵を復号するためのワーク鍵などを含むメッセージであり、共通情報(ECM:Entitlement Control Message)と対比して個別情報とも呼ばれる。なお、ECMは、番組情報やライセンス(コンテンツ鍵)などの全ユーザに共通の情報を含むメッセージである。EMMはユーザ個別に対して送信されるので、本実施形態におけるドメイン外利用条件付加部104は、EMMにドメイン外利用条件502を付加するものとしている。なお、ドメイン外利用条件付加部104は、EMMにドメイン外利用条件502を付加する代わりに他のメッセージ又は専用のメッセージにドメイン外利用条件502を付加するようにしてもよい。

[0056] ドメイン情報蓄積部105は、ドメインを管理するため、ユーザとドメインに属する端末装置及びICカードとを関連付けるドメイン情報テーブルを有するデータベースであって、図6に示すように、ドメインID601と、ユーザID602と、端末リスト603と、ICカードリスト604を含む。ドメインID601はドメインを一意に特定する識別子である。ユーザID602は、ドメインを使用するユーザの識別子である。端末リスト603は、ドメインに属する端末装置200を示す端末装置IDの一覧表である。ICカードリスト604は、ドメインに属するICカード300を特定するICカードIDの一覧表である。ICカードリスト604は、ドメインに属するICカードを特定するICカードIDのリストである。ドメイン情報テーブルへの端末装置200およびICカード300の登録は、会員登録後に随時行われる。なお、ドメイン情報テーブルは、ドメインID毎に当該ドメインの名称やニックネームを含んでいてもよい。また、ドメインは、端末装置のIDおよびICカードIDによってドメインを定義(以下論理的なドメインと呼ぶ。)してもよいし、端末装置の存在する位置によってドメインを定義(以下物理的なドメインと呼ぶ。)してもよい。図6に示したドメイン

情報テーブルは論理的なドメインの一例である。

[0057] 端末リスト付加部106は、EMM生成部107によって生成されユーザの端末装置に送信すべきEMMにドメイン情報蓄積部105に蓄積されるドメイン情報を付加する。これにより、EMMを受信した端末装置200およびICカード300はドメインの管理を行うことができる。

[0058] EMM生成部107は、上記のEMMを生成する。生成されたEMMには、ドメイン外利用条件付加部104によってドメイン外利用条件502が付加され、端末リスト付加部106によってドメイン情報が付加される。図7にEMMの一例を示す。同図のように、EMM700は、ヘッダ部701、EMM本体702、CRC704からなり、MPEG－2 Systems(IEC／ISO13818－1)のプライベートセクション形式のデータである。EMM本体702には、コンテンツ鍵402を復号するためのワーク鍵、プライベートデータ等の個別的な情報を含む。利用条件703は、ドメイン外利用条件付加部104によってEMM本体702内にプライベートデータとして付加されている。また、EMM本体702には、端末リスト付加部106によってプライベートデータとして端末リストも付加される。なお、EMM700は、ICカード300固有のマスタ鍵で暗号化される。

[0059] 放送信号多重送信部108は、EMM生成部107によって生成されたEMM700と、コンテンツ蓄積部101からの配信すべきコンテンツ等を多重化し放送する。これによる放送データは、デジタル放送の場合MPEG－2トランスポートストリーム(TS:Transport Stream)などの形式で送信される。多重化された放送データには、ECM等のセクション形式の種々のデータも含まれるが、本発明と関連が薄いデータについては説明を省略する。

[0060] 次に端末装置200の構成について説明する。図2に示すように、端末装置200は、図1における端末装置200a～200cの代表として1つだけ図示してある。この端末装置200は、放送信号受信分離部201、コンテンツ記憶部202、再生部203、EMM取得部204、端末ID読み出し部205、端末ID保持部206、ドメイン外利用条件取り出し部207、第1の送受信部208および制御部209を備える。

[0061] 放送信号受信分離部201は、配信装置100から送信される放送データを受信し、受信したデータからコンテンツと、ドメイン外利用条件502を含むEMM700と、その

他のPSI／SI(Program Specific Information／Service Information)等のセクション形式のデータとを分離する。

[0062] コンテンツ記憶部202は、放送信号受信分離部201によって分離されたコンテンツをパーシャルTSとして記憶する。なお、サーバ型放送のTypell(ファイル型)コンテンツであれば、タイムスタンプ付きTSやJPEGなどを蓄積する。

[0063] 再生部203は、コンテンツ記憶部202に記憶されたコンテンツを復号して再生する。コンテンツ記憶部202に記憶されたコンテンツは暗号化されているので、再生部203は、コンテンツ鍵と、コンテンツ鍵の暗号化を解くためのワーク鍵とを用いて復号化(デクリプト)し、さらにMPEG－2等に準拠した圧縮符号を伸張(デコード)する。そのため、再生部203はコンテンツ鍵をECMから取得するが、ワーク鍵はICカード300から第1の送受信部208を介して再生部203に供給される。

[0064] なお、ここでは、再生部203がコンテンツ鍵とワーク鍵とを用いて、コンテンツをデクリプトする場合の例を示したが、ICカード300にECMおよびEMMを復号するためのECM／EMM復号部を備え、ECM／EMM復号部においてECMおよびEMMを復号するようにしてもよい。この場合、ECM／EMM復号部でEMMを復号することによってワーク鍵を取得し、ワーク鍵をICカード内部で保持する。また、コンテンツを再生する場合には、再生部203がコンテンツに多重化されたECMをICカード300に送信し、ECM／EMM復号部がワーク鍵を用いてECMを復号することによってコンテンツ鍵を取得する。このように取得したコンテンツ鍵は、端末装置200に送信され、再生部203において、コンテンツ鍵を用いて暗号化コンテンツを復号する。

[0065] EMM取得部204は、放送信号受信分離部201によって分離されたEMM700を取得し、EMM本体702をドメイン外利用条件取り出し部207に出力する。

[0066] 端末ID読み出し部205は、端末ID保持部206に保持された端末装置200の端末IDを読み出して、第1の送受信部208を介してICカード300に出力する。

[0067] 端末ID保持部206は、端末装置200の端末ID情報を保持する。図8に、端末ID保持部206が保持する端末ID情報の一例を示す。図8の例では、端末ID情報800は、端末装置200を特定する端末ID801、端末装置200のユーザを特定するユーザID802、端末装置200が属するドメインを特定するドメインID803を含む。

[0068] ドメイン外利用条件取り出し部207は、端末装置200のICカードスロットにドメイン内のICカード300が挿入されている場合、EMM取得部204が取得したEMM本体702からドメイン外利用条件502や端末リスト603を取り出して内部に保持し、またEMM本体702を第1の送受信部208を介してICカード300に送信する。

[0069] 第1の送受信部208は、ICカードスロットに挿入されたICカード300と通信するためのインターフェースである。

[0070] 制御部209は、ドメイン内のICカード300から暗号鍵の供給を受けるための制御と、ドメイン外のICカード300からも暗号鍵の供給を受けるための制御を行う。ドメイン外のICカード300からは、ドメイン外利用条件502に従って暗号鍵が供給される。

[0071] 続いてICカード300の構成について説明する。ICカード300は、図1におけるICカード300a～300cの代表として1つだけ図示してある。図2に示すようにICカード300は、第2の送受信部301、ドメイン情報保持部302、端末ID取得部303、ドメイン情報処理部304、ドメイン外利用条件保持部305、ドメイン外利用条件取得部306、ドメイン外利用記録蓄積部307、ドメイン外利用記録更新部308、ドメイン外利用可否判定部309を備える。

[0072] 第2の送受信部301は、ICカード300が端末装置200のICカードスロットに挿入されたときに端末装置200と通信するためのインターフェースである。

[0073] ドメイン情報保持部302は、ICカード300のドメインに属する端末装置200を示すドメイン情報を保持する。このドメイン情報は端末IDリストを含み、ICカードIDリストは含まなくてもよいし、含んでもよい。図9に、ドメイン情報保持部302に保持されるドメイン情報の一例を示す。図9の例では、ドメイン情報900は、ICカード300が属するドメインを特定するドメインID901、ICカード300のユーザを特定するユーザID902、ドメインID901に特定されるドメインに属する端末装置200を示す端末リスト903とを含む。なお、合わせて、端末IDリストやICカードIDリストの登録数、期間、サイズなどの最大値を管理するようにしても良い。また、このとき、最大値に達した場合は、古いものや、利用頻度が少ないものから削除／上書きするようにすると良い。

[0074] 端末ID取得部303は、ICカード300が挿入された端末装置200の端末ID801を取得する。

[0075] ドメイン情報処理部304は、端末ID取得部303に取得された端末ID801がドメイン情報保持部302に保持された端末リスト903に含まれるか否かを判定する。つまり、ドメイン情報処理部304は、ICカード300を装着した端末装置200がドメイン内の端末装置200であるのかドメイン外の端末装置200であるのかを判定する。

[0076] ドメイン外利用条件保持部305は、端末装置200から第2の送受信部301およびドメイン外利用条件取得部306を介して取得されたドメイン外利用条件502を保持する。図10に、ドメイン外利用条件保持部305に保持されるドメイン外利用条件502の一例を示す。同図での例では、ドメイン外利用条件1000は、ドメイン外の端末装置200におけるコンテンツ利用可能範囲として「3回まで許可」という条件が保持されている。この場合、本ICカードのユーザは、ドメイン外の端末装置200において3回までコンテンツを利用することが可能となる。

[0077] ドメイン外利用条件取得部306は、端末装置200から第2の送受信部301を介して取得されたEMM本体702からワーク鍵、端末リストおよびドメイン外利用条件502を取得し、ワーク鍵、端末リストを内部に保持し、ドメイン外利用条件保持部305に格納する。

[0078] ドメイン外利用記録蓄積部307は、ドメイン外のコンテンツ利用装置におけるドメイン外利用条件502に基づいてコンテンツが利用されたとき、その利用記録をドメイン外利用履歴として蓄積する。図11に、利用記録の一例を示す。同図の例では、利用記録1100は、利用日時1101、ICカード300を使用したドメイン外の端末装置200を特定する端末ID1102、そのドメインを特定するドメインID1103、利用したライセンスを特定するためのライセンスID1104、実際に利用した時間を示す利用時間1105等を含む。

[0079] ドメイン外利用記録更新部308は、ドメイン外利用記録蓄積部307に対して利用記録(ドメイン外利用履歴)の消去と追加とを行う。具体的には、ドメイン外利用記録更新部308は、端末装置200からの消去指示を受けたとき、ドメイン外利用記録蓄積部307に蓄積された利用記録を端末装置200に送信した後に全て消去する。利用記録を消去する理由は、ユーザが、再度ICカード300のドメイン外での使用を、ドメイン外利用条件の範囲内で可能にするためである。また、ドメイン外利用記録更新部30

8は、ドメイン外の端末装置200におけるドメイン外利用条件502に基づくコンテンツの利用について、その利用記録をドメイン外利用記録蓄積部307に記録することにより利用記録を更新する。この利用記録は、例えば、図11に示した利用記録の1エントリーである。なお、ここでは、端末装置200からの消去指示を受けたとき、ドメイン外利用記録蓄積部307に蓄積された利用記録を、端末装置200に送信しているが、必ずしも送信しなくてもよい。

[0080] ドメイン外利用可否判定部309は、ドメイン情報処理部304によって、ICカード300を装着した端末装置200がドメイン外の端末装置200であると判定されたとき、当該端末装置がICカード300を利用可能か否か、を判定する。この判定は、ドメイン外利用記録蓄積部307に蓄積された利用記録が、ドメイン外利用条件に示される利用可能な範囲を超えないか否かによる。さらに、ドメイン外利用可否判定部309は、利用可能と判定した場合に、その旨を第2の送受信部301を介して装着先の端末装置200に通知するとともに、ドメイン外利用条件取得部306にワーク鍵を端末装置200に供給するように指示する。このワーク鍵の供給を受けることにより、ドメイン外の端末装置200において、コンテンツを再生することが可能となる。

[0081] 以上のように構成された本発明の実施の形態1におけるコンテンツ利用システムについて、以下、その動作を説明する。

[0082] 図12は、本コンテンツ利用システムにおいてICカード300にドメイン外利用条件を設定する処理を示すフローチャートである。同図のように、配信装置100においてEMM生成部107はEMM700を生成する(S101)。ドメイン外利用条件付加部104はドメイン外利用条件蓄積部103からEMM700の対象となるユーザに対応するドメイン外利用条件502を読み出して、生成されたEMM700に付加する(S102)。放送信号多重送信部108は、ドメイン外利用条件502が付加されたEMM700を、コンテンツとともに多重化して放送データとして端末装置200に送信する(S103)。

[0083] 端末装置200において、放送信号受信分離部201は放送データを受信し、EMM本体702を分離する(S201)。分離されたEMM本体702は、さらにEMM取得部204によってドメイン外利用条件取り出し部207、第1の送受信部208を介してICカード300に送信される(S202)。

[0084] ICカード300において、第2の送受信部301はEMM本体702を受信し、ドメイン外利用条件取得部306にそのEMM本体702出力する(S303)。ドメイン外利用条件取得部306は、EMM本体702からワーク鍵を取り出して内部に保持し、さらに、ドメイン外利用条件502を取り出して、ドメイン外利用条件保持部305に格納する(S304)。

[0085] このようにして配信装置100において事業者等が作成したドメイン外利用条件502が、EMM700に付加されることにより、端末装置200を経由してICカード300内に設定される。

[0086] 図13は、ICカード300が挿入された端末装置200において、ユーザが再生開始操作をしたときのコンテンツの再生処理を示すフローチャートである。同図のように、端末装置200において、端末ID読み出し部205は、端末ID保持部206から読み出した端末装置200が保持する端末ID801を、第1の送受信部208を介してICカード300に送信する(S210)。その後、第1の送受信部208がICカード300から暗号鍵(ワーク鍵)の供給を受けた場合(S211)、再生部203はワーク鍵を用いてコンテンツ鍵を復号し、復号されたコンテンツ鍵を用いてコンテンツを復号し、さらに平文となったコンテンツを再生する(S212)。

[0087] 一方、ICカード300において、第2の送受信部301を介して端末ID取得部303は端末ID801を受信する(S310)。ドメイン情報処理部304は、端末ID取得部303に取得された端末ID801がドメイン情報保持部302に保持された端末リスト903に含まれるか否かを判定することにより、ICカード300を装着された端末装置200がドメイン内の端末装置200であるのかドメイン外の端末装置200であるかを判定する(S311)。ドメイン情報処理部304によってドメイン内の端末装置200であると判定された場合、ドメイン外利用条件取得部306は保持しているワーク鍵を第2の送受信部301を介して端末装置200に供給する(S312)。

[0088] ドメイン情報処理部304によってドメイン外の端末装置200であると判定された場合、ドメイン外利用可否判定部309は、ドメイン外利用条件保持部305からドメイン外利用条件502を読み出し(S313)、ドメイン外利用記録蓄積部307からドメイン外利用履歴(利用記録1100)を読み出し(S314)、当該端末装置200でのICカード300の

利用可否を判定する(S315)。利用不可と判定された場合、ICカード300はこの処理を終わる。利用可能と判定された場合、ドメイン外利用条件取得部306は保持しているワーク鍵を第2の送受信部301を介して端末装置200に供給する(S316)。さらにドメイン外利用記録更新部308はドメイン外利用記録蓄積部307の利用記録を更新する(S317)。この更新のために、ドメイン外利用記録更新部308は、端末装置200における再生動作の終了したコンテンツについて端末装置200から再生時間、コンテンツID、ライセンスID等を取得して、利用記録1100を生成する。さらに、ドメイン外利用記録更新部308は、更新後の利用記録およびドメイン外利用条件502を第2の送受信部301を介して端末装置200に送信し、端末装置200に利用記録をユーザに表示することを指示する(S318)。この指示に従って、端末装置200では、送信されたコンテンツ外利用条件および利用記録に基づいてドメイン外の端末装置200における利用状況に関するガイダンスを表示するようにしてもよい。

[0089] このような処理より、ユーザがICカード300をドメイン外の端末装置200に挿入した場合でも、ドメイン外利用条件の範囲内で当該端末装置200においてコンテンツを視聴することができる。

[0090] 図14は、端末装置200及びICカード300における利用記録の消去処理を示すフローチャートである。端末装置200において、第1の送受信部208はICカードスロットにICカード300が新たに挿入されたかどうかを判定する(S220)。新たに挿入されたと判定された場合、第1の送受信部208は、端末ID読み出し部205によって端末ID保持部206から読み出された端末ID801を送信するとともに、ICカード300から送信されるICカードIDを受信する(S221)。その後、第1の送受信部208がICカード300から利用記録1100を受信した場合(S222)(端末装置200とICカード300とが同じドメインに属する場合)、制御部209は、第1の送受信部208を介してICカード300に利用記録1100の消去指示を送信する(S223)。さらに、制御部209は、利用記録1100に基づいてドメイン外の端末装置200における利用状況に関するガイダンスを表示する(S224)。

[0091] 一方、ICカード300において、第2の送受信部301はICカードスロットにICカード300が新たに挿入されたかどうかを判定する(S320)。新たに挿入されたと判定された

場合、第2の送受信部301は、ICカードIDを端末装置200に送信するとともに、端末装置200から送信される端末ID801を受信する(S321)。さらにドメイン情報処理部304は、第2の送受信部301および端末ID取得部303を介して受信された端末ID801と、ドメイン情報保持部302に保持された端末リスト903とを比較して、ICカード300を装着した端末装置200がドメイン内の端末装置200であるのかドメイン外の端末装置200であるかを判定する(S322)。ドメイン外と判定された場合、ICカード300はこの消去処理を終わる。ドメイン内と判定された場合、ドメイン外利用記録更新部308は、ドメイン外利用記録蓄積部307から利用記録を読み出して(S323)、第2の送受信部301を介して端末装置200に送信する(S324)。さらに、第2の送受信部301が端末装置200から消去指示を受信した場合(S325)、ドメイン外利用記録更新部308はドメイン外利用記録蓄積部307内の利用記録1100を消去する(S326)。

[0092] このような消去処理により、ドメイン外の端末装置200でICカード300を使用しきった場合(ドメイン外利用条件が許す範囲を消耗した場合)に、二度と使用できなくなる事態を避けることができる。また、ドメイン外利用条件の許す範囲の全てを使いきっていない場合でも、ドメイン外利用条件の許す範囲を回復することができる。消去処理をドメイン内の端末装置200にICカード300が挿入された場合に行っているのは、ユーザがドメイン外の端末装置200で長期間にわたって(あるいは何度も繰り返し)ICカード300を使用することを防止している。これにより、ユーザはドメイン内の端末装置200でのICカード利用を原則としつつ、例外的にドメイン外の端末装置200でICカード300を使用することを可能にしている。

[0093] 以上説明してきたように、本発明の実施の形態1におけるコンテンツ利用システムによれば、ユーザはドメイン外利用条件の範囲内で、ICカード300をドメイン外の端末装置200でも使用することができるので、ユーザの利便性を向上させることができる。しかも、ドメイン外でのICカード300の使用は無制限ではなくドメイン外利用条件502によって制限されるので、コンテンツを提供する事業者の権利保護を図ることができる。

[0094] また、ドメイン外利用履歴の消去処理を適宜行うことにより、ユーザがドメイン内の端末装置200でICカード300を利用することを原則としつつ、例外的にドメイン外の端

末装置200でICカード300を使用することを可能にしている。

[0095] 次に、本実施の形態におけるコンテンツ利用システムの変形例について説明する。

[0096] なお、上記実施の形態1では、ドメイン外利用記録更新部308とドメイン外利用可否判定部309はICカード300内に備えられているが、これらのいずれかを端末装置200内に備える構成としてもよい。前者の場合は、既存の端末装置200に対して少ない変更量で本発明を適用することでき、後者の場合は、既存のICカード300に対して少ない変更量で本発明を適用することができる。また、端末装置200およびICカード300の両方に備える構成としても良い。

[0097] なお、上記実施の形態では、デジタル放送のEMMを用いてドメイン外利用条件をICカード300に設定する場合の例を示したが、これに限られるものではなく、デジタル放送のECM(Kc伝送用ECM、ECM－Kw、ECM－Kc)やACI(Account Control Information)、Kc伝送用EMM、グループ宛てEMMなどを用いてドメイン外利用条件をICカード300に設定してもよいし、インターネットなどの通信経由で設定しても良い。またICカード300に限らず、端末装置200に設定するようにしても良い。

[0098] また、上記実施の形態では、ICカード300が同じドメイン内のどの端末装置200のICカードスロットに挿入されたときでも、前記利用記録を消去するが、同じドメイン内の特定の端末装置200のICカードスロットに挿入されたときのみ消去するように構成してもよい。その場合、図14のステップS223における消去指示の送信は、端末ID801とICカードIDなどを用いて、特定の端末装置200のみが行い、他の端末装置200は行わないように構成すればよい。

[0099] さらに、特定ドメインの特定端末装置200が、ドメイン内かドメイン外かに関わらずICカードに消去指示を送信するようにしてもよい。

[0100] また、上記実施の形態では、ICカード300を端末装置200のICカードスロットに挿入したときにドメイン外利用履歴を消去するようにしたが、これに限らず、端末装置200あるいはICカード300において、コンテンツやライセンスを利用した時点でドメイン外利用履歴を消去するようにしても良い。このときのコンテンツやライセンスは、特定コンテンツや特定ライセンスに限定してもよい。

[0101] また、ドメイン外利用記録更新部308は、端末装置200からの消去指示がなくても、利用記録1100を消去するようにしてもよい。例えば、1ヶ月に1回など、定期的に消去したり、ドメイン内の端末装置200でのコンテンツ利用がN回(例えば10回)なされる毎に消去するようにしてもよい。この場合、消去の頻度をドメイン外利用条件502の程度に応じて定めればよい。なお、この場合の消去の頻度を、ドメイン外利用条件502で指定するようにしてもよい。

[0102] また、ドメイン外利用履歴の消去にあたっては、通信や放送を介して、配信装置100が消去指示をおこなうようにしても良い。この場合、ICカード300がドメイン内の端末装置200に挿入されている場合のみに、ドメイン外利用履歴を消去するようにしても良い。

[0103] なお、上記実施の形態では、ドメイン外利用条件502は配信装置100から端末装置200を介してICカード300に設定されているが、ドメイン外利用条件保持部305はデフォルト(あらかじめ出荷時などに設定されていてもよいし、または、特定の方法により内部で生成してもよい)のドメイン外利用条件を保持するようにしてもよいし、端末装置200がデフォルトで保持するドメイン外利用条件の設定を受けるようにしてもよい。

[0104] また、図13のステップS318における利用記録1100の表示指示を受けて、端末装置200は、次のようなガイダンス表示をしてもよい。

[0105] (a)ドメイン外利用条件およびドメイン外利用履歴(利用記録)に基づいてドメイン外の端末装置200における利用状況に関するガイダンス、

[0106] (b)利用記録がドメイン外利用条件に示される利用可能範囲に達しているとき、利用記録の消去を促すガイダンス、

[0107] (c)利用記録の消去方法を示すヘルプメッセージ記したガイダンス(例えば、「端末装置AAAにICカードを挿入して消去してください」)、

[0108] (d)利用記録とドメイン外利用条件に示される利用可能範囲との差分が一定以下のとき、その旨示すガイダンス(例えば、「ドメイン外ではあと1回だけ利用可能」「ドメイン外ではコンテンツAのみ利用可能」「ドメイン外ではドメインBでのみ利用可能」など)

[0109] (e)利用記録とドメイン外利用条件に示される利用可能範囲との差分を示すガイダン

ス、

[0110] (f)利用記録がドメイン外利用条件に示される利用可能範囲に達したとき、その旨をガイダンス(例えば「これ以上ドメイン外では利用できません」)、

[0111] (g)利用記録とドメイン外利用条件に示される利用可能範囲との差分が小さくなるに連れて、ガイダンス表示の大きさおよび色の少なくとも一方を変化させる、

[0112] (h)利用状況に応じて端末装置200に備えられた発光部および音声出力部の少なくとも一方の出力態様をガイダンスとして変化させる、

[0113] (i)外部から更新可能なスケジュールに従ってガイダンスを表示すること(例えば1ヶ月ごと、起動時、ICカードIDの登録時/削除時、ICカードの挿入時など)、

[0114] (j)ICカードの状態を示すガイダンス(例えば、ICカード内の記憶容量、そのうちの空き容量、設定されているプロファイル(ユーザID、ドメインID、ICカードIDなど)、保持されているライセンス数(コンテンツ鍵あるいはワーク鍵数)、コンテンツを保持するための空き容量など)

[0115] (k)ICカード300と端末装置200とが異なるドメインに属する旨のガイダンス。

[0116] なお、上記(a)～(k)のメッセージ表示は、ユーザ操作に基づいて行うようにしても良い。さらに、端末装置200またはICカード300が属するドメインIDまたはドメイン名称を表示するようにしても良い。また、あるドメインに属する端末装置200またはICカード300の一覧を表示するようにしても良い。これらの表示タイミングは、端末装置200の起動時、ICカード300の挿抜時、端末装置200またはICカード300のドメインへの登録/ドメインからの削除時、端末装置200とICカード300の属するドメインが異なる場合、などが考えられる。

[0117] また、ドメインへの端末装置200またはICカード300の登録/削除を促すメッセージを表示するようにしても良い。

[0118] また、図14のステップS222において消去指示を送信しない場合に、ステップS224において上記(a)～(k)のガイダンス表示を行ってもよい。

[0119] また、端末装置200またはICカード300は、上記各ガイダンス用の複数メッセージを予め記憶する記憶部を有していてもよいし、デジタル放送や通信経由で、放送局101から動的に更新できるようにしても良い。あるいは、ユーザ設定によって更新でき

るようにしても良い

[0120] なお、図13のステップS316において、ICカード300は、コンテンツ鍵を供給するようにしてもよい。また、ワーク鍵を供給しないで利用可能というメッセージだけを応答することにより、端末装置200とICカード300の組で利用可能かどうかを確認する手段として用いてもよい。

[0121] また、ドメインを構成する端末装置200またはICカード300において、ドメインへの所属を有効期限で管理するようにしてもよい。

[0122] また、上記発明の実施形態では、全ての端末装置102およびICカード300において、ドメイン外利用条件502による制御を適用する場合の例を示したが、このような制御の対象外である端末装置200、ICカード300、もしくは、複数の端末装置200あるいはICカード300で構成するグループを設けるようにしても良い。

[0123] なお、端末装置200またはICカード300でライセンス管理する場合に、ドメイン内で取得したライセンスとドメイン外で取得したライセンスとを区別するようにしてもよい。また、端末装置200またはICカード300は、ドメイン外でのライセンスの取得を抑制するようにしても良い。但し、ここでのライセンスとは、少なくとも、コンテンツの利用条件とコンテンツ鍵とを含むデータ構造のことを指す。

[0124] また、ドメイン外利用条件保持部305は、複数のドメイン外利用条件502を保持してもよいし、この場合に、ドメイン外利用可否判定部309が状況に応じて選択するようにしてもよい。例えば、ドメイン毎やコンテンツ毎にドメイン外利用条件502を選択すればよい。また、ドメイン外利用可否判定部309が複数のドメイン外利用条件502を選択し、アンド条件またはオア条件として判定してもよい。

[0125] さらに、ドメイン外利用可否判定部309は、状況に応じて、ドメイン外利用条件を厳しくまたは緩く解釈して、利用可否を判定するようにしてもよい。このときのドメイン外利用条件502の解釈は、例えば、ドメイン外利用条件を示す数値を5割増しや5割引きした数値に換算すればよい。また、上記状況とは、端末装置200またはICカード300が保持するライセンス、コンテンツ、プログラムや、加入しているサービス、端末装置200やICカード300の種類／機能（グレード）、または、ユーザ操作などを含むものとする。

[0126] また、同一ドメインに属する端末装置200あるいはICカード300の間で、連携することにより、ドメイン外利用条件やドメイン外利用履歴を共有、交換するようにしても良い。

[0127] また、上記実施の形態では、端末装置200とICカード300とをバインドする場合の例を示したが、本発明は、端末装置200上で動作する特定プログラムをICカード300とをバインドする場合や、端末装置200とICカード300上の特定プログラムとをバインドする場合や、端末装置200上の特定プログラムとICカード上の特定プログラムとをバインドする場合にも適用することができるのは言うまでもない。

[0128] なお、上記実施の形態では、放送局100で端末装置200とICカード300のドメイン制御(ドメイン登録／削除)をおこなう場合の例を示したが、放送局100でドメイン制御をおこなわず、全てローカルでおこなう方法も可能であるし、端末装置200同士またはICカード300同士のドメイン制御は放送局100で行うものの、端末装置200とICカード300のドメイン制御、端末装置200とICカード300の組の利用可否制御については、ローカルでおこなう方法も可能である。具体的には、

[0129] (A)共通情報(暗号鍵やIDなど)を保持する端末装置200とICカード300を同一ドメインとする。共通情報の設定／削除は、デジタル放送や通信でおこなってもよいし、ローカルで行ってもよい。

[0130] (B)ICカード300を端末装置200に最初に挿入したときに自動的にドメイン登録をおこなう。ドメイン登録の方法は、共通情報を共有する方法でも良いし、端末IDリストまたはICカードリストに、端末IDまたはICカードIDを追加する方法でも良い。

[0131] (C)最初にコンテンツまたはライセンスを、利用または取得した端末装置200とICカード300を同一ドメインとする(ドメイン登録する)。

[0132] (D)端末装置200へのICカード300の挿抜回数、挿入期間で制御する。なお、この場合、端末装置200へのICカード300の挿入時や端末装置200の電源投入時などの、コンテンツを利用するタイミング以外に、ドメイン外利用条件判定を行うようにしてもよい。

などがあげられる。

[0133] また、ドメイン制御について、ICカード300で保持するライセンスあるいはコンテンツ

に応じて、端末装置200とICカード300とのバインドを変更するようにしても良いし、利用するライセンスあるいはコンテンツによっても、端末装置200とICカード300とのバインドを変更するようにしても良い。

[0134] また、端末装置200同士またはICカード300同士が構築するドメインに連動して、端末装置200とICカード300との間のドメイン制御(利用可能な組の制御)をおこなうようにしても良い。

[0135] また、ドメイン制御に必要な情報(共通情報や端末IDリスト、ICカードリスト)は、ホームネットワークに属する他の端末装置200あるいはICカード300から取得／同期するようにしてもよい。

[0136] また、ドメイン制御に必要な情報は、デジタル放送や通信経由で、放送局101から動的に指示できるようにしてもよく、特に、放送局101からのドメインへの登録／削除指示を受信した時点で、端末装置200に挿入されているICカード300と関連付けをおこなうようにしてもよい。通信の場合は、SAC(Secure Authenticated Channel)により、セキュアに登録／削除をおこなえばよい。

[0137] (実施の形態2)

本実施の形態におけるセキュアシステムは、企業内あるいは家庭内のシステムなどに本発明を適用する場合について説明する。また、ドメインは、端末装置の存在する位置などによって定義された物理的なドメインを用いる例を説明する。

[0138] 図15は、本発明の実施の形態2におけるセキュアシステムの概要を示す図である。同図のように、本セキュアシステムは、端末装置Ta～Tc、端末装置Tp、Tq、セキュアデバイスとしてメモリカードCa～Ccを含み、ユーザがドメイン内の端末装置だけでなく、条件付でドメイン外の端末装置でメモリカードを使用できるように構成されている。

[0139] 同図のドメインC、Dは、物理的に定義されたドメインであり、例えば、企業内の事業所と事業所B、A棟とB棟、部署Aと部署B、学校内の校舎Aと校舎B、1学年の教室と2学年の教室、ネットワークAに接続された端末群とネットワークBに接続された端末群、などである。

[0140] 端末Taは、パーソナルコンピュータPC、モバイル機器(携帯電話機、PDAなど)な

どであり、メモリカードにセキュアに秘匿データを読み書きする。また、実施の形態1に示したコンテンツ利用端末や、セキュリティモジュール(ICカード)を利用してデジタル放送を受信するためのセットトップボックス、デジタルTV、DVDレコーダ、ハードディスクレコーダ、パーソナルコンピュータなどのコンテンツ再生装置、記録装置)であってもよい。他の端末Tb等についても同様である。

[0141] メモリカードCaは、秘匿データをセキュアに保持するセキュアデバイスの一種である。例えば、SDカード、メモリスティックといったセキュリティ保護機能付きメモリカードや、smartSDカード、MOPASS(MObile PASS port)カードといったICカード機能付きメモリカードなどがある。秘匿データは、コンテンツの暗号鍵に限らず、機密文書や、暗号化されたコンテンツ(動画、音声、静止画など)などである。

[0142] 図16は、端末装置Taとメモリカードの構成を示すブロック図である。同図の端末装置Taは、図2の端末装置200と比較して、放送信号受信分離部201、コンテンツ記憶部202、再生部203、EMM取得部204が削除されている点と、GPS部210が追加されている点と、端末ID読み出し部205の代わりに読み出し部205aを備える点と、ドメイン外利用条件取り出し部207の代わりにドメイン外利用条件記憶部部207aを備える点とが異なる。また、同図のメモリカードCaは、図2のICカード300と比較して、ほぼ同様に構成されているが、ドメイン情報保持部302に保持されるドメイン定義情報が異なっている。以下、同じ点は説明を省略して異なる点を中心に説明する。

[0143] GPS部210は、GPS(Global Positioning System)システムから端末装置の位置を検出する。検出される位置は、緯度、経度、高度などで表される。

[0144] 読み出し部205aは、端末ID読み出し部205の機能に加えて、GPS部210によって検出された位置を示す情報を、端末IDと共に第1の送受信部208を介してメモリカードCaに出力する。

[0145] ドメイン外利用条件記憶部207aは、ドメイン外利用条件を保持する。ドメイン外利用条件は実施の形態1と同様である。

[0146] ドメイン情報保持部302は、物理的に定義されたドメインを示すドメイン情報を保持する。

[0147] 図17は、ドメイン情報保持部302に保持されるドメイン情報の例を示す図である。

同図のドメイン情報は、図9のドメイン情報と比較して、端末リストの代わりにドメイン定義データとして位置情報の組みが設定されている。例えば、位置情報の組みによって囲まれる範囲に存在する端末装置はドメイン内と判定される。位置情報に高さが含まれる場合は3次元の範囲としてドメインが定義される。なお、位置情報と半径の組みによってドメインが定義されてもよい。

[0148] 図18は、ドメイン情報保持部302に保持されるドメイン情報の他の例を示す図である。同図のドメイン定義データは、ネットワークIDを含む。この場合、ネットワークIDで特定されるネットワークに接続されていること端末装置は、ドメイン内と判定される。

[0149] 本実施の形態におけるセキュアシステムが、会社の構内をドメインとする端末装置と、機密文書を保持するメモリカードとに適用される場合について説明する。

[0150] ユーザは原則として、会社の構内(ドメイン)において、会社の機密文書(秘匿データ)をメモリカード(セキュアデバイス)に記録し、会社が認定したセキュリティ対策済PC(端末装置Ta)で機密文書を利用する。会社の構内であることは、GPS部210により検出される位置に基づいて、ドメイン内であるかドメイン外であるかが判定される。ドメイン内かドメイン外かの判定の結果、会社の構内であれば、機密文書を自由に利用可能だが、会社の構内でない場合は、メモリカードCaに記録しておいた時間制限／回数制限(ドメイン外利用条件)により、機密文書へのアクセスが限定されるが、例外的に利用可能となる。

[0151] ドメイン外利用条件を使い切ってしまった場合、会社の構内でメモリカードを端末装置Taに挿入し、ドメイン内であることを確認できた時点で、ドメイン外利用条件がリセットされ、再度ドメイン外で利用可能な状態となる。

[0152] なお、物理的なドメイン定義は、例えば、GPSの利用により事前に登録された範囲、無線LAN、RFID(無線タグ)等の電波を受信できる範囲、特定ネットワークに接続されていることが確認できる端末装置、特定端末などから音や光が届く範囲、などとしてもよい。また、論理的なドメイン定義は、端末装置ID／セキュアデバイスIDのリスト以外でもよく、例えば、ドメイン鍵、ドメインID、リージョンコード、セキュアデバイスの挿抜回数／時間等で定義してもよい。また、これらは秘密にしていてもよい。

[0153] また、端末装置とセキュアデバイスとが同じドメインに属するかを判定する代わりに、

端末装置とセキュアデバイスのそれぞれについて自身のドメインに属しているかを判定するようにしてもよい。この判定の結果、一方のみがドメインに属している場合には、セキュアデバイスの利用可否判定をセキュアに行うため、端末装置とセキュアデバイスとの間で相互認証を行ってもよい。

[0154] なお、ドメイン情報保持部302は、ICカードCaだけでなく端末装置Taに備えられてもよいし、端末装置Taのみに備えられてもよい。

[0155] また、端末装置Ta等は、図2の端末装置200に示した放送信号？受信分離部201やコンテンツ記憶部202を備え、外部からコンテンツ等を受信および記憶する構成であってもよい。

[0156] なお、端末装置Ta等は、必ずしも端末IDを保持しなくてよく、端末ID読み出し部205を備えていなくてもよく、また、端末IDをメモリカードCa等に送信しなくてもよい。

[0157] また、実施の形態1のコンテンツ利用システムの各種変形例は、本実施の形態のセキュアシステムにも同様に適用できることはいうまでもない。

## 産業上の利用可能性

[0158] 本発明は、端末装置とセキュアデバイスとを含むセキュアシステムに適している。特に、セキュアデバイスを共用するコンテンツ利用装置からなるドメインに属するコンテンツ利用装置にコンテンツ利用を可能にする暗号鍵を供給するセキュアデバイスを利用するコンテンツ利用システム、セキュアデバイス、コンテンツ利用装置、方法およびプログラムに適していて、例えば、セキュリティモジュール(ICカード)を利用してデジタル放送を受信するためのセットトップボックス、デジタルTV、DVDレコーダ、ハードディスクレコーダ、パーソナルコンピュータなどのコンテンツ再生装置、記録装置あるいはこれらの複合機器等に適している。

# 請求の範囲

[1] 秘匿データを保持するセキュアデバイスと、セキュアデバイスを接続する端末装置とを含むセキュアシステムであって、

セキュアデバイスおよび端末装置の何れかに備えられ、セキュアデバイスおよび端末装置のドメインを定義するドメイン情報とを記憶する第1記憶手段と、

セキュアデバイスおよび端末装置の何れかに備えられ、ドメイン外におけるセキュアデバイスの利用条件であるドメイン外利用条件を記憶する第2記憶手段と、

セキュアデバイスおよび端末装置の何れかに備えられ、前記ドメイン情報に従ってセキュアデバイスまたは端末装置が現在ドメイン内であるかドメイン外であるかを判定する第1判定手段と、

セキュアデバイスおよび端末装置の何れかに備えられ、第1判定手段によってドメイン外であると判定されたとき、前記ドメイン外利用条件に従ってセキュアデバイスの利用可否を判定する第2判定手段と、

セキュアデバイスおよび端末装置の何れかに備えられ、第1判定手段によってドメイン内と判定された場合、および、第2判定手段によって利用可能と判定された場合に、端末装置によるセキュアデバイスの利用を可能にする制御手段と、

を備えることを特徴とするセキュアシステム。

[2] 前記端末装置は、暗号化されたコンテンツを再生するコンテンツ利用装置であり、

前記秘匿データは前記コンテンツを復号するための暗号鍵であり、

前記制御手段は、セキュアデバイスに備えられ、第1判定手段によってドメイン内と判定された場合、および、第2判定手段によって利用可能と判定された場合に、セキュアデバイスから端末装置に前記秘匿データを供給する

ことを特徴とする請求項1記載のセキュアシステム。

[3] 前記ドメイン外利用条件は、ドメイン外での(a)コンテンツ再生の回数、(b)コンテンツ利用装置の台数、(c)ドメイン数、(d)有効期限、(e)利用時間、(f)端末ID数、(g)ドメインID数、(h)コンテンツの数および(i)ライセンスの数、の少なくとも1つに関する

ことを特徴とする請求項2記載のセキュアシステム。

[4] 前記セキュアデバイスは、

ドメイン外のコンテンツ利用装置における前記ドメイン外利用条件に基づくコンテンツの利用履歴を示すドメイン外利用履歴を記録する履歴記録手段を備え、

前記第2判定手段は、前記ドメイン外利用履歴が前記利用条件に示される利用可能な範囲を超えないか否かを判定する

ことを特徴とする請求項2記載のセキュアシステム。

[5] 第2記憶手段および第2判定手段は、前記セキュアデバイスに備えられる

ことを特徴とする請求項2記載のセキュアシステム。

[6] 第2記憶手段および第2判定手段は、前記コンテンツ利用装置に備えられる

ことを特徴とする請求項2記載のセキュアシステム。

[7] 前記コンテンツ利用装置は、外部から新たなドメイン外利用条件を受信する受信手段を備え、

前記第2記憶手段は、前記ドメイン外利用条件を新たなドメイン外利用条件に更新する

ことを特徴とする請求項2記載のセキュアシステム。

[8] 前記受信手段は、コンテンツ配信サーバから送信されるライセンスに付加されたドメイン外利用条件を受信する

ことを特徴とする請求項7記載のセキュアシステム。

[9] 前記コンテンツ利用装置は、さらに、

セキュアデバイススロットに挿入されたセキュアデバイスから前記ドメイン外利用条件および前記ドメイン外利用履歴を取得する取得手段と、

取得した前記ドメイン外利用条件および前記ドメイン外利用履歴に基づいてドメイン外のコンテンツ利用装置における利用状況に関するガイダンスを表示する表示手段と

を備えることを特徴とする請求項2記載のセキュアシステム。

[10] 端末装置に接続され、秘匿データを保持するセキュアデバイスであって、

ドメイン外の端末装置に対するセキュアデバイスのドメイン外利用条件を記憶する条件記憶手段と、

前記ドメイン外利用条件に従ってセキュアデバイスの利用可否を判定する判定手

段と

判定手段によって利用可能と判定された場合に、端末装置によるセキュアデバイスの利用を可能にする制御手段と、

を備えることを特徴とするセキュアデバイス。

[11] 前記端末装置は、暗号化されたコンテンツを再生するコンテンツ利用装置であり、

前記秘匿データは前記コンテンツを復号するための暗号鍵であり、

前記制御手段は、セキュアデバイスに備えられ、判定手段によって利用可能と判定された場合に、セキュアデバイスから端末装置に前記秘匿データを供給する

ことを特徴とする請求項10記載のセキュアシステム。

[12] 前記ドメイン外利用条件は、(a)コンテンツ再生の回数、(b)コンテンツ利用装置の台数、(c)ドメイン数、(d)有効期限、(e)利用時間、(f)端末ID数、(g)ドメインID数、(h)コンテンツの数および(i)ライセンスの数、の少なくとも1つに関する

ことを特徴とする請求項11記載のセキュアデバイス。

[13] 前記セキュアデバイスは、

ドメイン外の端末装置における前記ドメイン外条件に基づくコンテンツの利用履歴を示す前記ドメイン外利用履歴を記録する履歴記録手段を備え、

前記判定手段は、前記ドメイン外利用履歴が前記ドメイン外利用条件に示される利用可能な範囲を超えないか否かを判定する

ことを特徴とする請求項12記載のセキュアデバイス。

[14] 前記セキュアデバイスは、さらに、所定の時期に前記ドメイン外利用履歴を消去する消去手段を備える

ことを特徴とする請求項13記載のセキュアデバイス。

[15] 前記セキュアデバイスは、端末装置から新たなドメイン外利用条件を受信する受信手段を備え、

前記条件記憶手段は、前記ドメイン外利用条件を新たなドメイン外利用条件に更新する

ことを特徴とする請求項11記載のセキュアデバイス。

[16] 条件記憶手段は、デフォルトのドメイン外利用条件を記憶する

ことを特徴とする請求項11記載のセキュアデバイス。

[17] 前記セキュアデバイスは、さらに、

前記ドメイン外利用条件および前記ドメイン外利用履歴に基づいてドメイン外のコンテンツ利用装置における利用状況提示する表示手段を有する

ことを特徴とする請求項11記載のセキュアデバイス。

[18] 前記セキュアデバイスは、さらに、

挿入されているセキュアデバイススロットの端末装置に、ドメインIDを送信する送信手段を備える

ことを特徴とする請求項11記載のセキュアデバイス。

[19] 前記セキュアデバイスは、さらに、

挿入されているセキュアデバイススロットの端末装置に、前記ドメイン外利用履歴を送信する送信手段を備える

ことを特徴とする請求項11記載のセキュアデバイス。

[20] 秘匿データを保持するセキュアデバイスを接続する端末装置であって、

ドメイン外の端末装置に対するセキュアデバイスの利用条件であるドメイン外利用条件を記憶する記憶手段と、

前記ドメイン外利用条件に従ってセキュアデバイスの利用可否を判定する判定手段と

判定手段によって利用可能と判定された場合に、端末装置によるセキュアデバイスの利用を可能にする制御手段と、

を備えることを特徴とする端末装置。

[21] 前記端末装置は、暗号化されたコンテンツを再生するコンテンツ利用装置であり、

前記秘匿データは前記コンテンツを復号するための暗号鍵であり、

前記制御手段は、セキュアデバイスに備えられ、判定手段によって利用可能と判定された場合に、セキュアデバイスから端末装置に前記秘匿データを供給する

ことを特徴とする請求項20記載のセキュアシステム。

[22] 前記ドメイン外利用条件は、(a)コンテンツ再生の回数、(b)コンテンツ利用装置の台数、(c)ドメイン数、(d)有効期限、(e)利用時間、(f)端末ID数、(g)ドメインID数、(

h)コンテンツの数および(i)ライセンスの数、の少なくとも1つに関する

ことを特徴とする請求項21記載の端末装置。

[23] コンテンツ配信装置とコンテンツ利用装置とセキュアデバイスとを含むセキュアシステムであって、

前記コンテンツ配信装置は、ドメイン外のコンテンツ利用装置に対するセキュアデバイスの利用条件であるドメイン外利用条件をコンテンツ利用装置に送信する送信手段を備え、

前記セキュアデバイスは、セキュアデバイスを共用するコンテンツ利用装置からなるドメインに属するコンテンツ利用装置に、コンテンツ利用を可能にする暗号鍵を供給する供給手段を備え、

前記コンテンツ利用装置は、前記送信手段から前記ドメイン外利用条件を受信する受信手段を備え、

前記コンテンツ利用装置およびセキュアデバイスの一方は、

セキュアデバイスおよび端末装置のドメインを定義するドメイン情報とを記憶する第1記憶手段と、

受信手段に受信された利用条件を記憶する第2記憶手段と、

前記ドメイン情報に従ってセキュアデバイスまたは端末装置が現在ドメイン内であるかドメイン外であるかを判定する第1判定手段と、

第1判定手段によってドメイン外であると判定されたとき、前記ドメイン外利用条件に従ってセキュアデバイスの利用可否を判定する第2判定手段と

を備え、

前記供給手段は、さらに、前記判定手段によって利用可と判定されたとき、ドメイン外のコンテンツ利用装置に暗号鍵を供給する

ことを特徴とするセキュアシステム。

[24] 秘匿データを保持するセキュアデバイスと、セキュアデバイスを接続する端末装置とを含むセキュアシステムにおけるセキュアデバイス利用方法であって、

セキュアデバイスおよび端末装置の何れかに備えられたメモリから、セキュアデバイスおよび端末装置のドメインを定義するドメイン情報を読み出すステップと、

読み出されたドメイン情報に従ってセキュアデバイスまたは端末装置が現在ドメイン内であるかドメイン外であるかを判定するステップと、

セキュアデバイスおよび端末装置の何れかに備えられたメモリから、ドメイン外におけるセキュアデバイスの利用条件であるドメイン外利用条件を読み出すステップと、

第1判定手段によってドメイン外であると判定されたとき、読み出されたドメイン外利用条件に従ってセキュアデバイスの利用可否を判定するステップと、

ドメイン内と判定された場合、および、利用可能と判定された場合に、端末装置によるセキュアデバイスの利用を可能にする制御ステップと、

を備えることを特徴とするセキュアデバイス利用方法。

[25] 前記端末装置は、暗号化されたコンテンツを再生するコンテンツ利用装置であり、

前記秘匿データは前記コンテンツを復号するための暗号鍵であり、

前記制御ステップにおいて、セキュアデバイスに備えられ、第1判定手段によってドメイン内と判定された場合、および、第2判定手段によって利用可能と判定された場合に、セキュアデバイスから端末装置に前記秘匿データを供給する

ことを特徴とする請求項24記載のセキュアデバイス利用方法。

[26] 秘匿データを保持するセキュアデバイスと、セキュアデバイスを接続する端末装置とを含むセキュアシステムにおけるコンピュータ実行可能なプログラムであって、

前記プログラムは、

セキュアデバイスおよび端末装置の何れかに備えられたメモリから、セキュアデバイスおよび端末装置のドメインを定義するドメイン情報を読み出すステップと、

読み出されたドメイン情報に従ってセキュアデバイスまたは端末装置が現在ドメイン内であるかドメイン外であるかを判定するステップと、

セキュアデバイスおよび端末装置の何れかに備えられたメモリから、ドメイン外におけるセキュアデバイスの利用条件であるドメイン外利用条件を読み出すステップと、

第1判定手段によってドメイン外であると判定されたとき、読み出されたドメイン外利用条件に従ってセキュアデバイスの利用可否を判定するステップと、

ドメイン内と判定された場合、および、利用可能と判定された場合に、端末装置によるセキュアデバイスの利用を可能にするステップと、

をコンピュータに実行させることを特徴とするプログラム。

をコンピュータに実行させることを特徴とするプログラム。

[27] コンテンツ配信装置とコンテンツ利用装置とセキュアデバイスとを含むコンテンツ利用システムにおけるコンテンツ配信装置であって、

ドメイン外のコンテンツ利用装置に対するセキュアデバイスの利用条件であるドメイン外利用条件をコンテンツ利用装置に送信する送信手段を備える

ことを特徴とするコンテンツ配信装置。

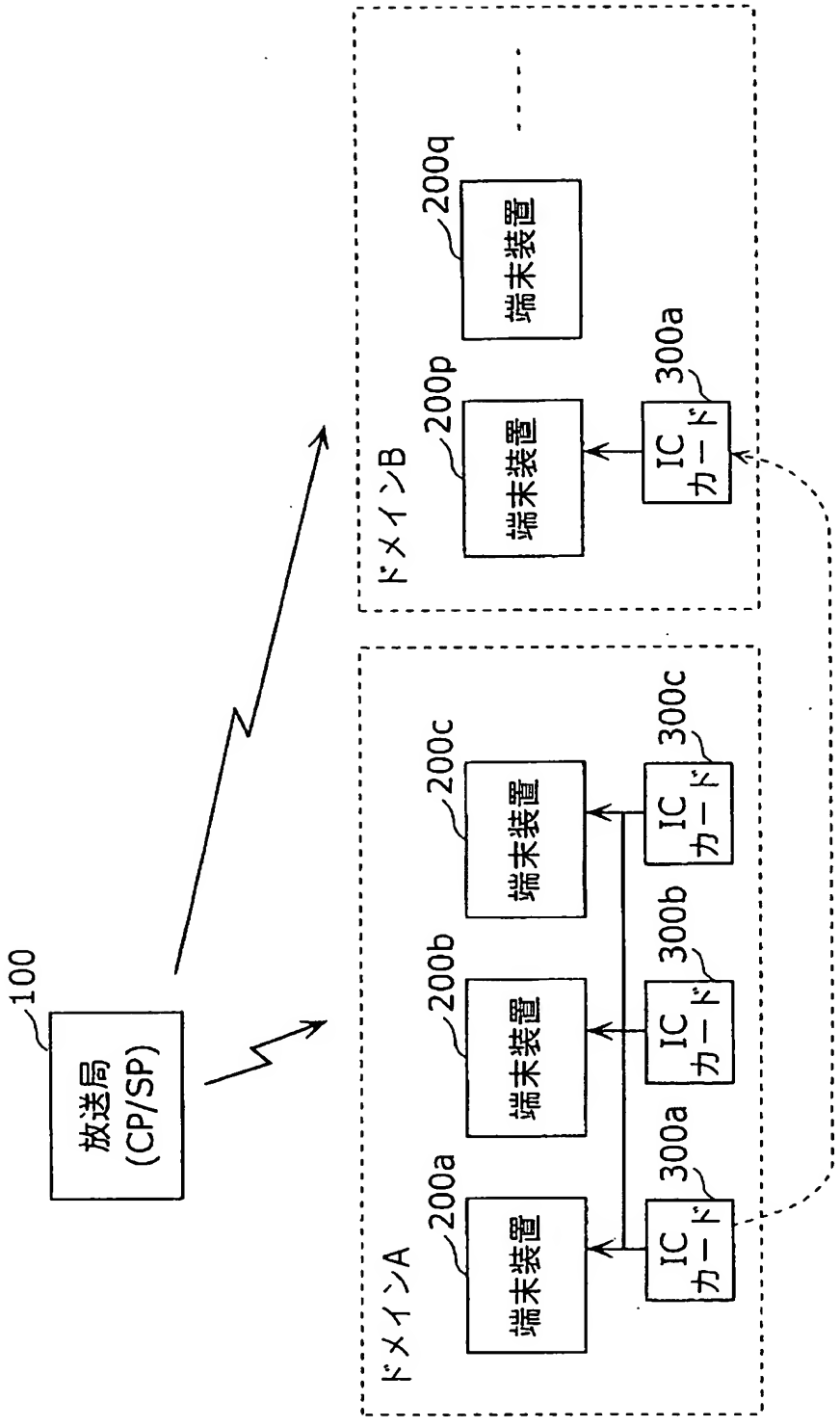
[28] 前記ドメイン外利用条件は、ドメイン外での(a)コンテンツ再生の回数、(b)コンテンツ利用装置の台数、(c)ドメイン数、(d)有効期限、(e)利用時間、(f)端末ID数、(g)ドメインID数、(h)コンテンツの数および(i)ライセンスの数、の少なくとも1つに関する

ことを特徴とする請求項27記載のコンテンツ配信装置。

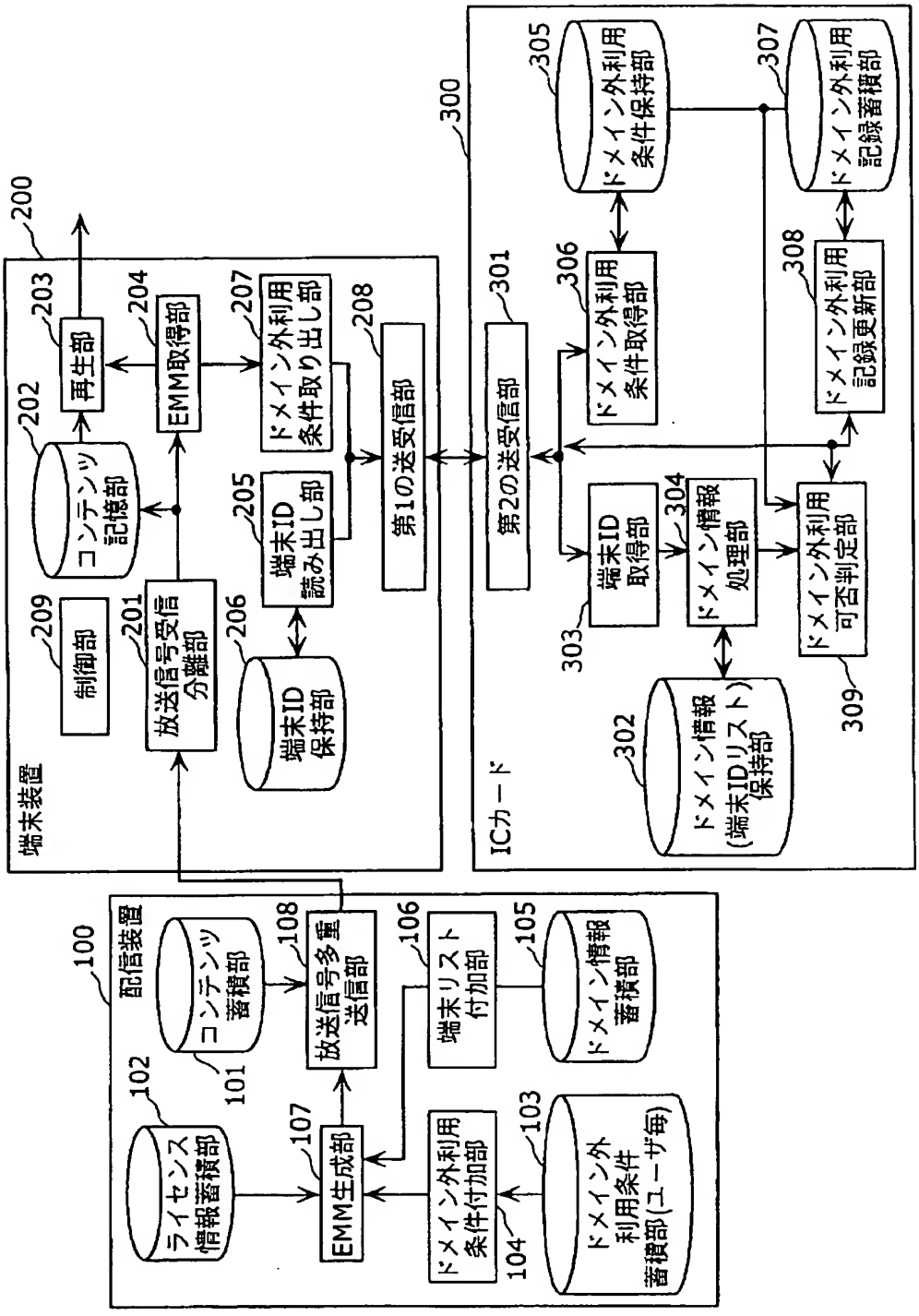
# 要 約 書

ICカード300は、ICカード300を共用する端末装置か200らなるドメインに属する端末装置200に、コンテンツ利用を可能にする暗号鍵を供給し、ICカード300は、ドメイン外の端末装置200に対するICカード300の利用条件を記憶するドメイン外利用条件保持部305と、ICカード300が端末装置200に装着されたとき、利用条件に従ってICカード300の利用可否を判定するドメイン外利用可否判定部309とを備え、ICカード300は、さらに、ドメイン外利用可否判定部309によって利用可と判定されたとき、ドメイン外の端末装置200に暗号鍵を供給する。

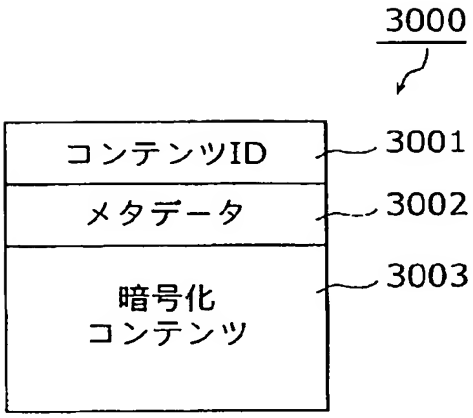
[図1]


100
放送局
(CP/SP)
ドメインA
200a
端末装置
300a
ICカード
200b
端末装置
300b
ICカード
200c
端末装置
300c
ICカード
ドメインB
200p
端末装置
300a
ICカード
200q
端末装置

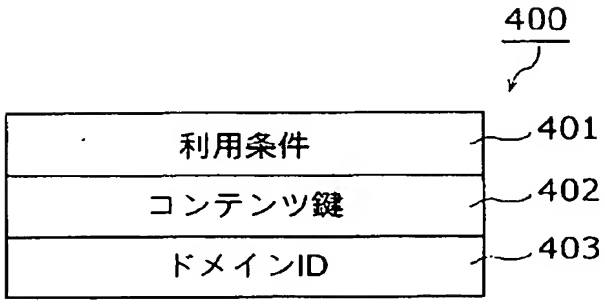
[図2]


100
配信装置
101
コンテンツ蓄積部
102
ライセンス情報蓄積部
103
ドメイン外利用条件蓄積部(ユーザ毎)
104
ドメイン外利用条件付加部
105
ドメイン情報蓄積部
106
端末リスト付加部
107
EMM生成部
108
放送信号多重送信部
200
端末装置
201
放送信号受信分離部
202
コンテンツ記憶部
203
再生部
204
EMM取得部
205
端末ID読み出し部
206
端末ID保持部
207
ドメイン外利用条件取り出し部
208
第1の送受信部
209
制御部
300
ICカード
301
第2の送受信部
302
ドメイン情報(端末IDリスト)保持部
303
端末ID取得部
304
ドメイン情報処理部
305
ドメイン外利用条件保持部
306
ドメイン外利用条件取得部
307
ドメイン外利用記録蓄積部
308
ドメイン外利用記録更新部
309
ドメイン外利用可否判定部

[図3]




[図4]

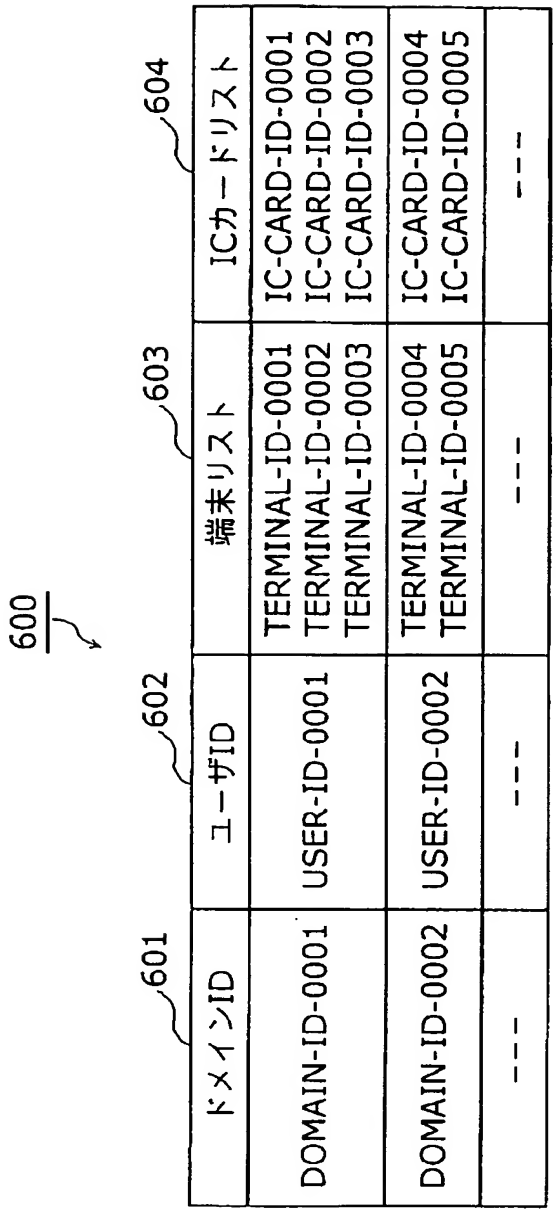



[図5]

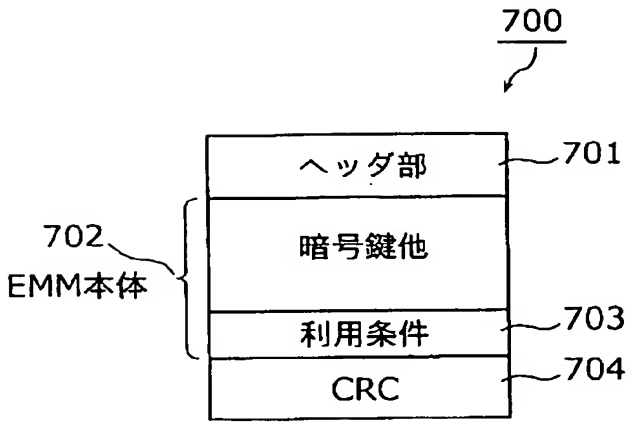
500

| 501 ユーザID | 502 ドメイン外利用条件 |
|---|---|
| USER-ID-0001 | 端末ID3つまで許可 |
| USER-ID-0002 | 3つまで許可 |
| USER-ID-0003 | 初回利用から1カ月経過後無効 |
| ― ― ― | ― ― ― |

[図6]


600
601
602
603
604
ドメインID
ユーザID
端末リスト
ICカードリスト
DOMAIN-ID-0001
USER-ID-0001
TERMINAL-ID-0001
TERMINAL-ID-0002
TERMINAL-ID-0003
IC-CARD-ID-0001
IC-CARD-ID-0002
IC-CARD-ID-0003
DOMAIN-ID-0002
USER-ID-0002
TERMINAL-ID-0004
TERMINAL-ID-0005
IC-CARD-ID-0004
IC-CARD-ID-0005
---
---
---
---

[図7]




[図8]

800

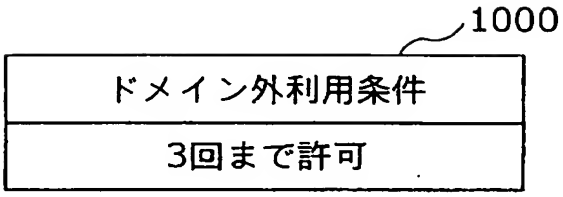
| 801 端末ID | 802 ユーザID | 803 ドメインID |
|---|---|---|
| TERMINAL-ID-0001 | USER-ID-0001 | DOMAIN-ID-0001 |

[図9]

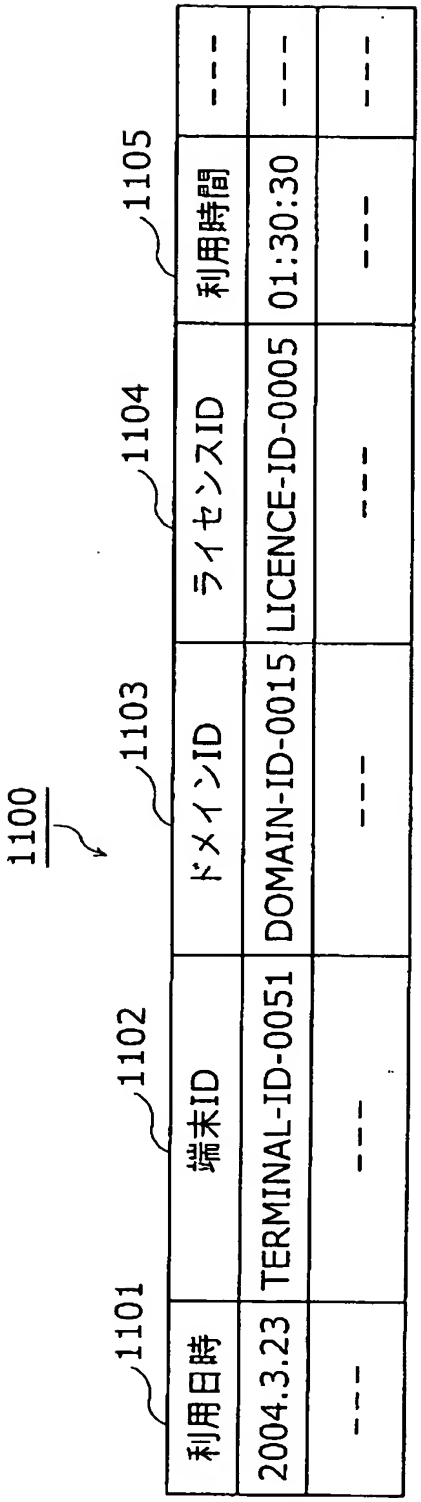
900

| 901 ドメインID | 902 ユーザID | 903 端末リスト |
|---|---|---|
| DOMAIN-ID-0001 | USER-ID-0001 | TERMINAL-ID-0001<br>TERMINAL-ID-0002<br>TERMINAL-ID-0003 |

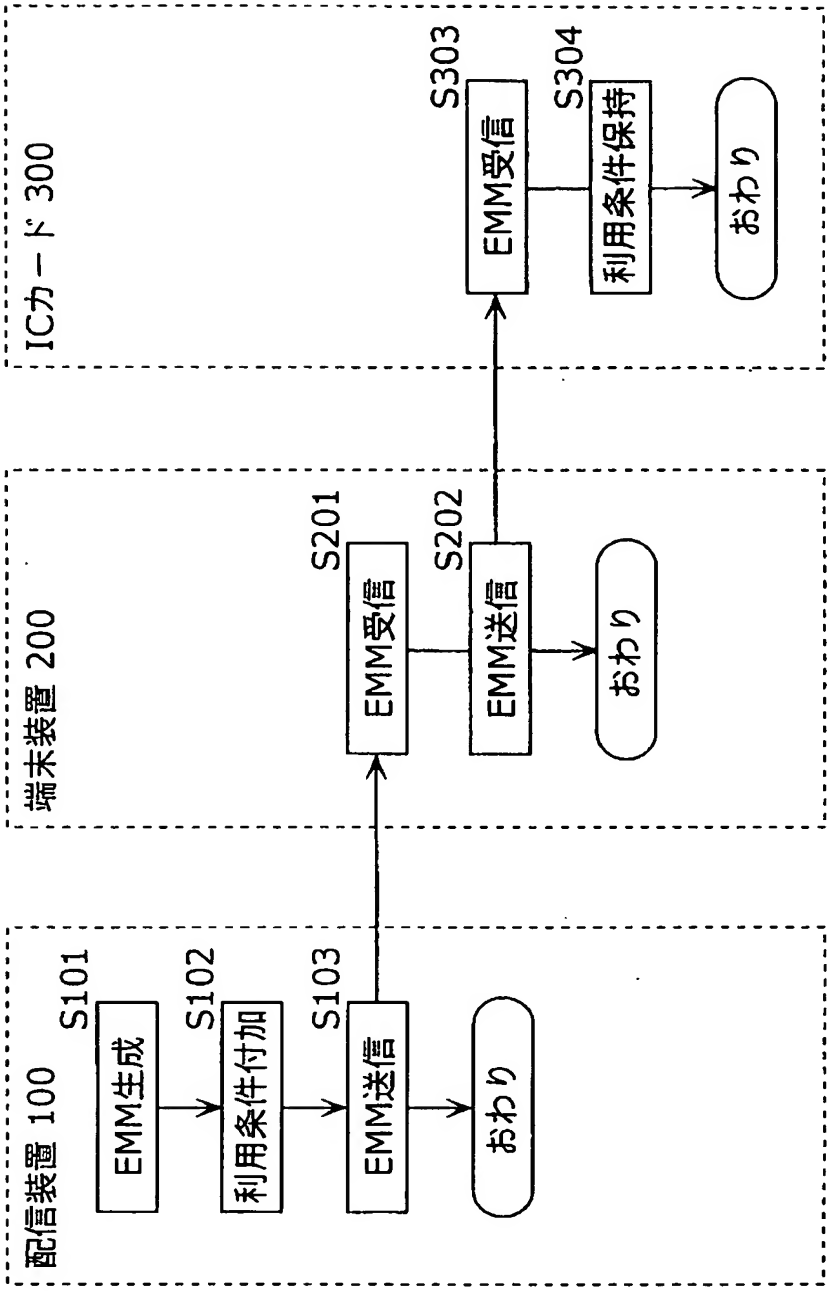
[図10]



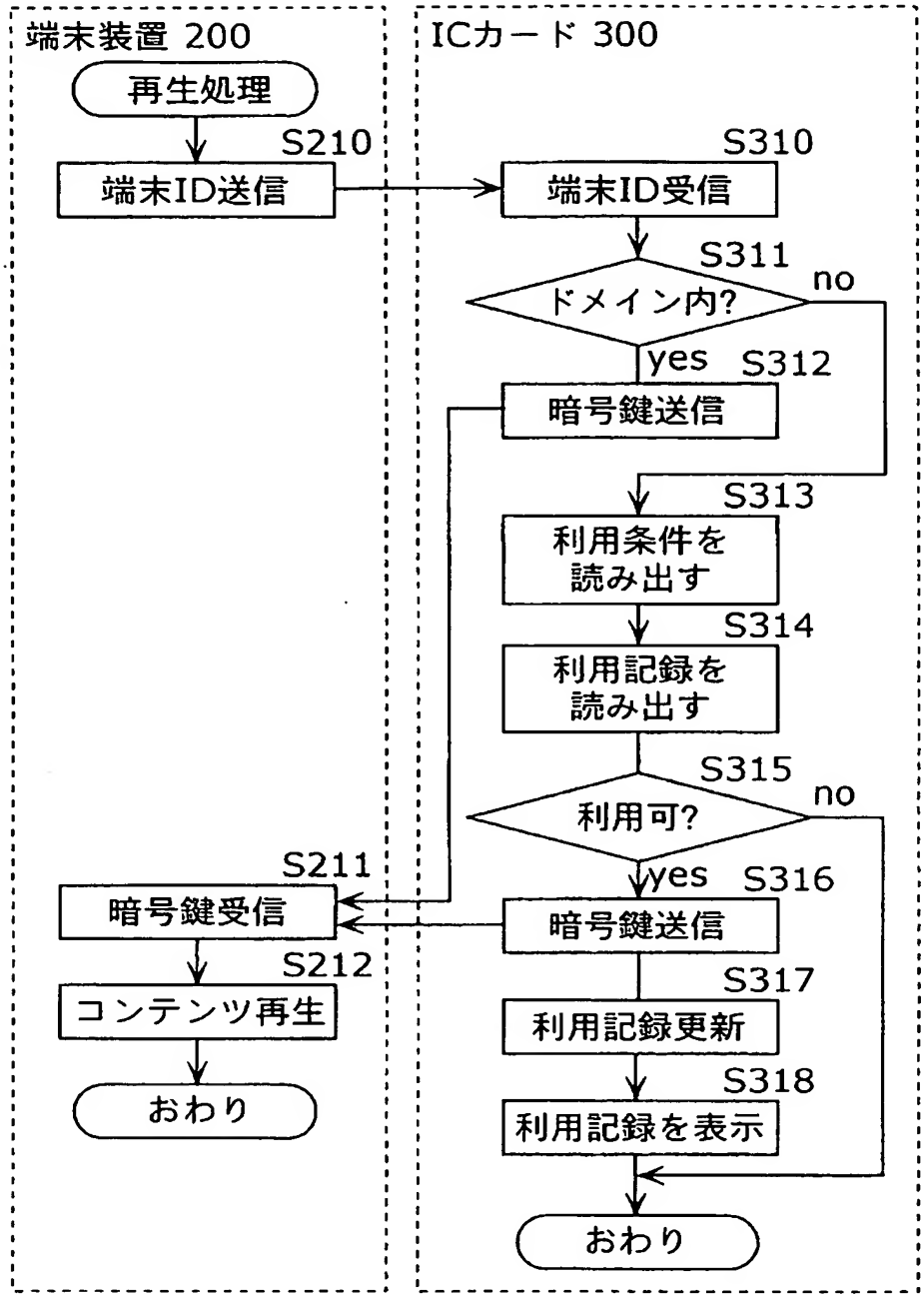
[図11]


1100
1101
利用日時
2004.3.23
---
1102
端末ID
TERMINAL-ID-0051
---
1103
ドメインID
DOMAIN-ID-0015
---
1104
ライセンスID
LICENCE-ID-0005
---
1105
利用時間
01:30:30
---
---
---
---
---
---
---

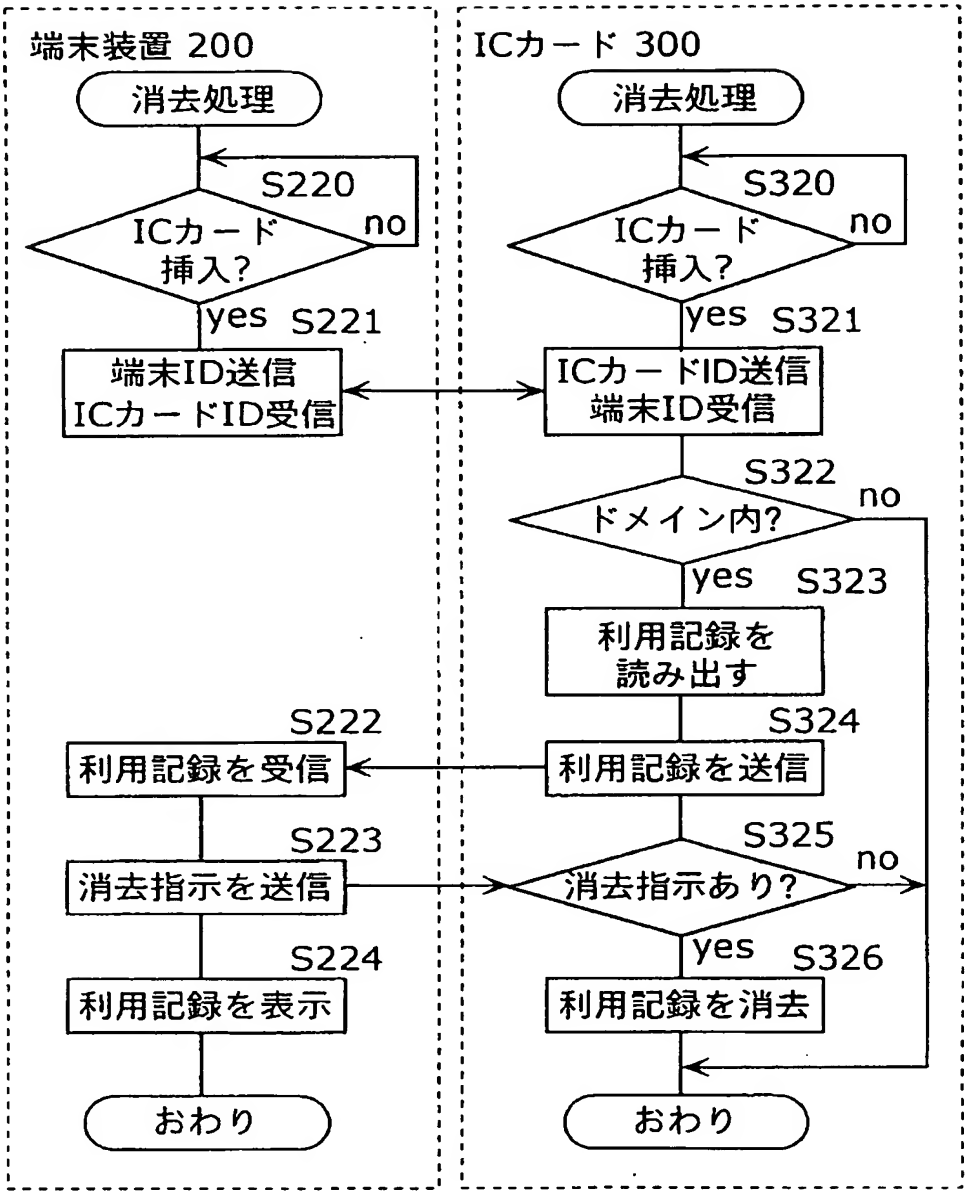
[図12]


配信装置 100
S101
EMM生成
S102
利用条件付加
S103
EMM送信
おわり
端末装置 200
S201
EMM受信
S202
EMM送信
おわり
ICカード 300
S303
EMM受信
S304
利用条件保持
おわり

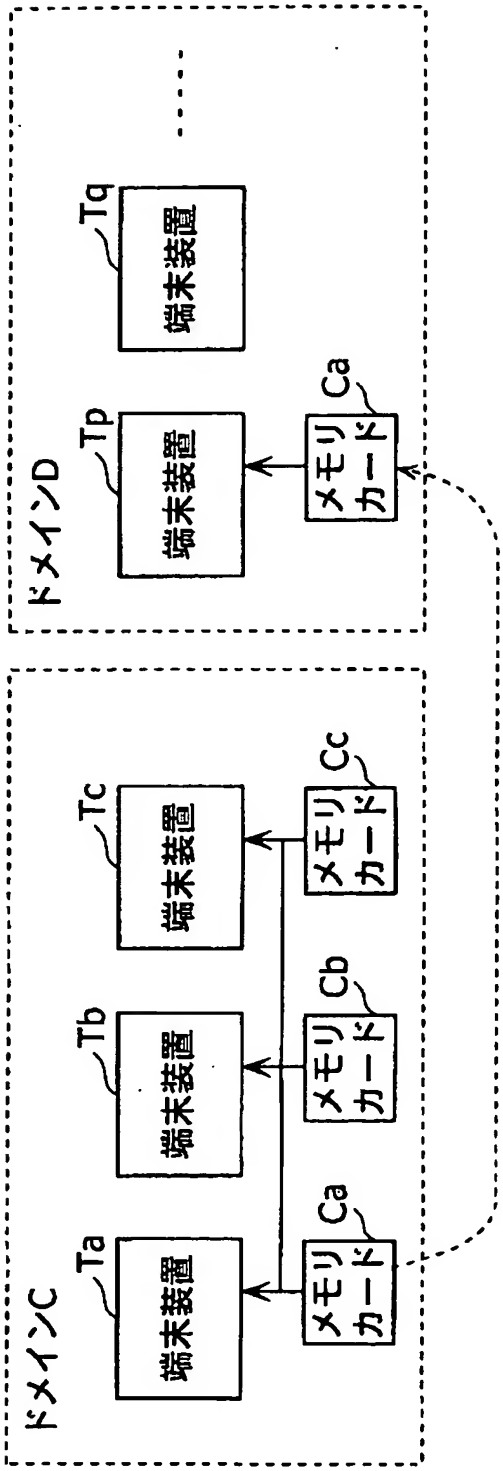
[図13]


端末装置 200
ICカード 300
再生処理
S210
端末ID送信
S310
端末ID受信
S311
ドメイン内?
no
yes
S312
暗号鍵送信
S313
利用条件を
読み出す
S314
利用記録を
読み出す
S315
利用可?
no
yes
S316
暗号鍵送信
S317
利用記録更新
S318
利用記録を表示
おわり
S211
暗号鍵受信
S212
コンテンツ再生
おわり

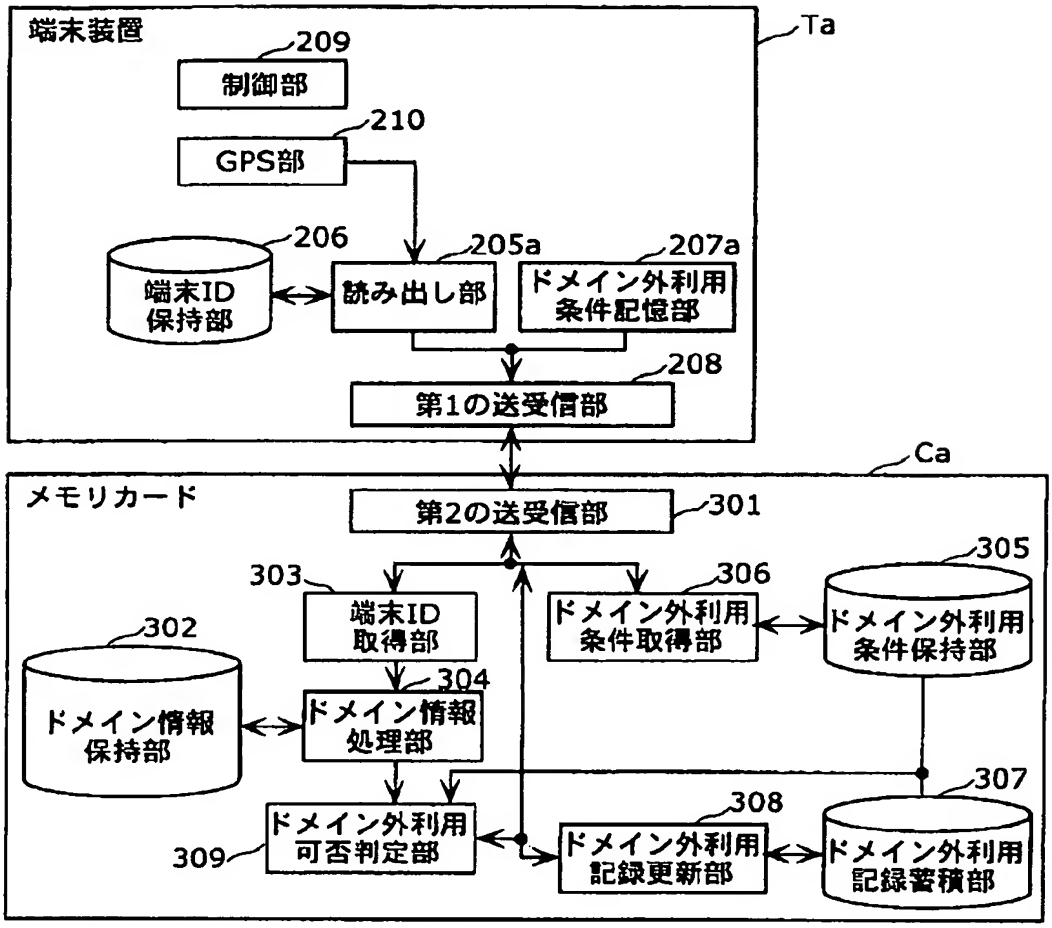
[図14]


端末装置 200
消去処理
S220
ICカード
挿入?
no
yes
S221
端末ID送信
ICカードID受信
S222
利用記録を受信
S223
消去指示を送信
S224
利用記録を表示
おわり
ICカード 300
消去処理
S320
ICカード
挿入?
no
yes
S321
ICカードID送信
端末ID受信
S322
ドメイン内?
no
yes
S323
利用記録を
読み出す
S324
利用記録を送信
S325
消去指示あり?
no
yes
S326
利用記録を消去
おわり

[図15]


ドメインC
Ta
端末装置
Tb
端末装置
Tc
端末装置
Ca
メモリカード
Cb
メモリカード
Cc
メモリカード
ドメインD
Tp
端末装置
Tq
端末装置
Ca
メモリカード

[図16]

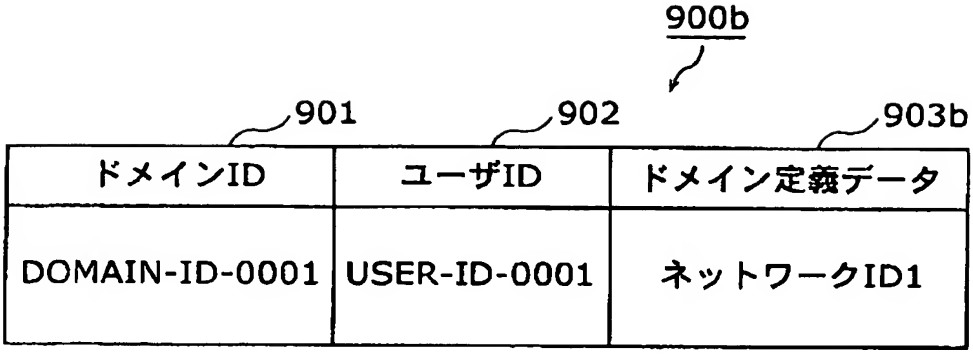



[図17]

900a

| 901 ドメインID | 902 ユーザID | 903a ドメイン定義データ |
|---|---|---|
| DOMAIN-ID-0001 | USER-ID-0001 | 位置情報1<br>位置情報2<br>⋮ |

[図18]


900b
901
902
903b
ドメインID
ユーザID
ドメイン定義データ
DOMAIN-ID-0001
USER-ID-0001
ネットワークID1